

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Risk management – Risk assessment techniques

Management du risque – Techniques d'appréciation du risque

for more information please follow

@jefriimron
@jeapconsultant

Jeap Consultant Library



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2019 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC -

webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.



IEC 31010

Edition 2.0 2019-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Risk management – Risk assessment techniques

Management du risque – Techniques d'appréciation du risque

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.100.01

ISBN 978-2-8322-6989-3

Warning! Make sure that you obtained this publication from an authorized distributor. Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.
--

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	9
2 Normative references	9
3 Terms and definitions	9
4 Core concepts	10
4.1 Uncertainty	10
4.2 Risk	11
5 Uses of risk assessment techniques	11
6 Implementing risk assessment.....	12
6.1 Plan the assessment.....	12
6.1.1 Define purpose and scope of the assessment	12
6.1.2 Understand the context.....	13
6.1.3 Engage with stakeholders.....	13
6.1.4 Define objectives	13
6.1.5 Consider human, organizational and social factors	13
6.1.6 Review criteria for decisions	14
6.2 Manage information and develop models	16
6.2.1 General	16
6.2.2 Collecting information	16
6.2.3 Analysing data.....	16
6.2.4 Developing and applying models	17
6.3 Apply risk assessment techniques.....	18
6.3.1 Overview	18
6.3.2 Identifying risk	19
6.3.3 Determining sources, causes and drivers of risk	19
6.3.4 Investigating the effectiveness of existing controls.....	20
6.3.5 Understanding consequences, and likelihood	20
6.3.6 Analysing interactions and dependencies	22
6.3.7 Understanding measures of risk.....	22
6.4 Review the analysis	25
6.4.1 Verifying and validating results	25
6.4.2 Uncertainty and sensitivity analysis	25
6.4.3 Monitoring and review.....	26
6.5 Apply results to support decisions.....	26
6.5.1 Overview	26
6.5.2 Decisions about the significance of risk	27
6.5.3 Decisions that involve selecting between options.....	27
6.6 Record and report risk assessment process and outcomes	28
7 Selecting risk assessment techniques.....	28
7.1 General.....	28
7.2 Selecting techniques.....	29
Annex A (informative) Categorization of techniques	31
A.1 Introduction to categorization of techniques	31
A.2 Application of categorization of techniques	31
A.3 Use of techniques during the ISO 31000 process.....	37

Annex B (informative) Description of techniques	40
B.1 Techniques for eliciting views from stakeholders and experts.....	40
B.1.1 General	40
B.1.2 Brainstorming	40
B.1.3 Delphi technique.....	42
B.1.4 Nominal group technique	43
B.1.5 Structured or semi-structured interviews	44
B.1.6 Surveys	45
B.2 Techniques for identifying risk.....	46
B.2.1 General	46
B.2.2 Checklists, classifications and taxonomies.....	47
B.2.3 Failure modes and effects analysis (FMEA) and failure modes, effects and criticality analysis (FMECA)	49
B.2.4 Hazard and operability (HAZOP) studies.....	50
B.2.5 Scenario analysis	52
B.2.6 Structured what if technique (SWIFT)	54
B.3 Techniques for determining sources, causes and drivers of risk	55
B.3.1 General	55
B.3.2 Cindynic approach	56
B.3.3 Ishikawa analysis (fishbone) method	58
B.4 Techniques for analysing controls	60
B.4.1 General	60
B.4.2 Bow tie analysis.....	60
B.4.3 Hazard analysis and critical control points (HACCP).....	62
B.4.4 Layers of protection analysis (LOPA).....	64
B.5 Techniques for understanding consequences and likelihood	66
B.5.1 General	66
B.5.2 Bayesian analysis.....	66
B.5.3 Bayesian networks and influence diagrams.....	68
B.5.4 Business impact analysis (BIA).....	70
B.5.5 Cause-consequence analysis (CCA).....	72
B.5.6 Event tree analysis (ETA)	74
B.5.7 Fault tree analysis (FTA)	76
B.5.8 Human reliability analysis (HRA).....	78
B.5.9 Markov analysis.....	79
B.5.10 Monte Carlo simulation	81
B.5.11 Privacy impact analysis (PIA) / data protection impact analysis (DPIA).....	83
B.6 Techniques for analysing dependencies and interactions	85
B.6.1 Causal mapping.....	85
B.6.2 Cross impact analysis.....	87
B.7 Techniques that provide a measure of risk	89
B.7.1 Toxicological risk assessment.....	89
B.7.2 Value at risk (VaR)	91
B.7.3 Conditional value at risk (CVaR) or expected shortfall (ES)	93
B.8 Techniques for evaluating the significance of risk	94
B.8.1 General	94
B.8.2 As low as reasonably practicable (ALARP) and so far as is reasonably practicable (SFAIRP)	94

B.8.3	Frequency-number (F-N) diagrams	96
B.8.4	Pareto charts	98
B.8.5	Reliability centred maintenance (RCM)	100
B.8.6	Risk indices	102
B.9	Techniques for selecting between options	103
B.9.1	General	103
B.9.2	Cost/benefit analysis (CBA)	104
B.9.3	Decision tree analysis	106
B.9.4	Game theory	107
B.9.5	Multi-criteria analysis (MCA)	109
B.10	Techniques for recording and reporting	111
B.10.1	General	111
B.10.2	Risk registers	112
B.10.3	Consequence/likelihood matrix (risk matrix or heat map)	113
B.10.4	S-curves	117
	Bibliography	119
	Figure A.1 – Application of techniques in the ISO 31000 risk management process [3]	37
	Figure B.1 – Example Ishikawa (fishbone) diagram	59
	Figure B.2 – Example of Bowtie	61
	Figure B.3 – A Bayesian network showing a simplified version of a real ecological problem: modelling native fish populations in Victoria, Australia	69
	Figure B.4 – Example of cause-consequence diagram	73
	Figure B.5 – Example of event tree analysis	75
	Figure B.6 – Example of fault tree	77
	Figure B.7 – Example of Markov diagram	80
	Figure B.8 – Example of dose response curve	89
	Figure B.9 – Distribution of value	91
	Figure B.10 – Detail of loss region VaR values	91
	Figure B.11 – VaR and CVaR for possible loss portfolio	93
	Figure B.12 – ALARP diagram	95
	Figure B.13 – Sample F-N diagram	97
	Figure B.14 – Example of a Pareto chart	98
	Figure B.15 – Part example of table defining consequence scales	114
	Figure B.16 – Part example of a likelihood scale	114
	Figure B.17 – Example of consequence/likelihood matrix	115
	Figure B.18 – Probability distribution function and cumulative distribution function	117
	Table A.1 – Characteristics of techniques	31
	Table A.2 – Techniques and indicative characteristics	32
	Table A.3 – Applicability of techniques to the ISO 31000 process	38
	Table B.1 – Examples of basic guidewords and their generic meanings	51

Table B.2 – Table of deficits for each stakeholder	57
Table B.3 – Table of dissonances between stakeholders	57
Table B.4 – Example of Markov matrix	80
Table B.5 – Examples of systems to which Markov analysis can be applied	81
Table B.6 – An example of RCM task selection	101
Table B.7 – Example of a game matrix	108

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**RISK MANAGEMENT –
RISK ASSESSMENT TECHNIQUES****FOREWORD**

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 31010 has been prepared by IEC technical committee 56: Dependability, in co-operation with ISO technical committee 262: Risk management.

It is published as a double logo standard.

This second edition cancels and replaces the first edition published in 2009. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- more detail is given on the process of planning, implementing, verifying and validating the use of the techniques;
- the number and range of application of the techniques has been increased;
- the concepts covered in ISO 31000 are no longer repeated in this standard.

The text of this International Standard is based on the following documents of IEC:

FDIS	Report on voting
56/1837/FDIS	56/1845/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table. In ISO, the standard has been approved by 44 P members out of 46 having cast a vote.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This document provides guidance on the selection and application of various techniques that can be used to help improve the way uncertainty is taken into account and to help understand risk.

The techniques are used:

- where further understanding is required about what risk exists or about a particular risk;
- within a decision where a range of options each involving risk need to be compared or optimized;
- within a risk management process leading to actions to treat risk.

The techniques are used within the risk assessment steps of identifying, analysing and evaluating risk as described in ISO 31000, and more generally whenever there is a need to understand uncertainty and its effects.

The techniques described in this document can be used in a wide range of settings, however the majority originated in the technical domain. Some techniques are similar in concept but have different names and methodologies that reflect the history of their development in different sectors. Techniques have evolved over time and continue to evolve, and many can be used in a broad range of situations outside their original application. Techniques can be adapted, combined and applied in new ways or extended to satisfy current and future needs.

This document is an introduction to selected techniques and compares their possible applications, benefits and limitations. It also provides references to sources of more detailed information.

The potential audience for this document is:

- anyone involved in assessing or managing risk;
- people who are involved in developing guidance that sets out how risk is to be assessed in specific contexts;
- people who need to make decisions where there is uncertainty including:
 - those who commission or evaluate risk assessments,
 - those who need to understand the outcomes of assessments, and
 - those who have to choose assessment techniques to meet particular needs.

Organizations that are required to conduct risk assessments for compliance or conformance purposes would benefit from using appropriate formal and standardized risk assessment techniques.

RISK MANAGEMENT – RISK ASSESSMENT TECHNIQUES

1 Scope

This International Standard provides guidance on the selection and application of techniques for assessing risk in a wide range of situations. The techniques are used to assist in making decisions where there is uncertainty, to provide information about particular risks and as part of a process for managing risk. The document provides summaries of a range of techniques, with references to other documents where the techniques are described in more detail.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO Guide 73:2009, *Risk management – Vocabulary*

ISO 31000:2018, *Risk management – Guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 31000:2018, ISO Guide 73:2009 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1

likelihood

chance of something happening

Note 1 to entry: In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

[SOURCE: ISO 31000:2018, 3.7]

3.2

opportunity

combination of circumstances expected to be favourable to objectives

Note 1 to entry: An opportunity is a positive situation in which gain is likely and over which one has a fair level of control.

Note 2 to entry: An opportunity to one party may pose a threat to another.

Note 3 to entry: Taking or not taking an opportunity are both sources of risk.

3.3 probability

measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty

Note 1 to entry: See definition 3.1, Note 2 to entry.

3.4 risk driver driver of risk

factor that has a major influence on risk

3.5 threat

potential source of danger, harm, or other undesirable outcome

Note 1 to entry: A threat is a negative situation in which loss is likely and over which one has relatively little control.

Note 2 to entry: A threat to one party may pose an opportunity to another.

4 Core concepts

4.1 Uncertainty

Uncertainty is a term which embraces many underlying concepts. Many attempts have been made, and continue to be developed, to categorize types of uncertainty including:

- uncertainty which recognizes the intrinsic variability of some phenomena, and that cannot be reduced by further research; for example, throwing dice (sometimes referred to as aleatory uncertainty);
- uncertainty which generally results from a lack of knowledge and that therefore can be reduced by gathering more data, by refining models, improving sampling techniques, etc. (sometimes referred to as epistemic uncertainty).

Other commonly recognized forms of uncertainty include:

- linguistic uncertainty, which recognizes the vagueness and ambiguity inherent in spoken languages;
- decision uncertainty, which has particular relevance to risk management strategies, and which identifies uncertainty associated with value systems, professional judgement, company values and societal norms.

Examples of uncertainty include:

- uncertainty as to the truth of assumptions, including presumptions about how people or systems might behave;
- variability in the parameters on which a decision is to be based;
- uncertainty in the validity or accuracy of models which have been established to make predictions about the future;
- events (including changes in circumstances or conditions) whose occurrence, character or consequences are uncertain;
- uncertainty associated with disruptive events;
- the uncertain outcomes of systemic issues, such as shortages of competent staff, that can have wide ranging impacts which cannot be clearly defined;

- lack of knowledge which arises when uncertainty is recognized but not fully understood;
- unpredictability;
- uncertainty arising from the limitations of the human mind, for example in understanding complex data, predicting situations with long-term consequences or making bias-free judgments.

Not all uncertainty is able to be understood and the significance of uncertainty might be hard or impossible to define or influence. However, a recognition that uncertainty exists in a specific context enables early warning systems to be put in place to detect change in a proactive and timely manner and make arrangements to build resilience to cope with unexpected circumstances.

4.2 Risk

Risk includes the effects of any of the forms of uncertainty described in 4.1 on objectives. The uncertainty may lead to positive or negative consequences or both.

Risk is often described in terms of risk sources, potential events, their consequences and their likelihoods. An event can have multiple causes and lead to multiple consequences. Consequences can have a number of discrete values, be continuous variables or be unknown. Consequences may not be discernible or measurable at first, but may accumulate over time. Sources of risk can include inherent variability, or uncertainties related to a range of factors including human behaviour and organizational structures or societal influences for which it can be difficult to predict any particular event that might occur. It follows that risk cannot always be tabulated easily as a set of events, their consequences and their likelihoods.

Risk assessment techniques aim to help people understand uncertainty and the associated risk in this broad, complex and diverse context, for the purpose of supporting better-informed decisions and actions.

5 Uses of risk assessment techniques

The techniques described in this document provide a means to improve understanding of uncertainty and its implications for decisions and actions.

ISO 31000 describes principles for managing risk and the foundations and organizational arrangements that enable risk to be managed. It specifies a process that enables risk to be recognized, understood and modified as necessary, according to criteria that are established as part of the process. Risk assessment techniques can be applied within this structured approach which involves establishing context, assessing risk and treating risk, along with ongoing monitoring, review, communication and consultation, recording and reporting. This process is illustrated in Figure A.1 which also shows examples of where within the process techniques can be applied.

In the ISO 31000 process, risk assessment involves identifying risks, analysing them, and using the understanding gained from the analysis to evaluate risk by drawing conclusions about their comparative significance in relation to the objectives and performance thresholds of the organization. This process provides inputs into decisions about whether treatment is required, priorities for treatment and the actions intended to treat risk. In practice an iterative approach is applied.

Risk assessment techniques described in this document are used

- where further understanding is required about what risks exist or about a particular risk;
- within a risk management process leading to actions to treat risk;
- within a decision where a range of options each involving risk needs to be compared or optimized.

In particular, the techniques can be used to:

- provide structured information to support decisions and actions where there is uncertainty;
- clarify the implications of assumptions on the achievement of objectives;
- compare multiple options, systems, technologies or approaches, etc. where there is multifaceted uncertainty around each option;
- assist in defining realistic strategic and operational objectives;
- help determine an organization's risk criteria, such as risk limits, risk appetite or risk bearing capacity;
- take risk into account when setting or reviewing priorities;
- recognize and understand risk, including risk that could have extreme outcomes;
- understand which uncertainties matter most to an organization's objectives and provide a rationale for what should be done about them;
- recognize and exploit opportunities more successfully;
- articulate the factors that contribute to risk and why they are important;
- identify effective and efficient risk treatment actions;
- determine the modifying effect of proposed risk treatments, including any change in the nature or magnitude of risk;
- communicate about risk and its implications;
- learn from failure and successes in order to improve the way risk is managed;
- demonstrate that regulatory and other requirements have been satisfied.

The way in which risk is assessed depends on the situation's complexity and novelty, and the level of relevant knowledge and understanding.

- In the simplest case, when there is nothing new or unusual about a situation, risk is well understood, with no major stakeholder implications or consequences are not significant, then actions are likely to be decided according to established rules and procedures and previous assessments of risk.
- For very novel, complex or challenging issues, where there is high uncertainty and little experience, there is little information on which to base assessment and conventional techniques of analysis might not be useful or meaningful. This also applies to circumstances where stakeholders hold strongly divergent views. In these cases, multiple techniques might be used to gain a partial understanding of risk, with judgements then made in the context of organizational and societal values, and stakeholder views.

The techniques described in this document have greatest application in situations between these two extremes where the complexity is moderate and there is some information available on which to base the assessment.

6 Implementing risk assessment

6.1 Plan the assessment

6.1.1 Define purpose and scope of the assessment

The purpose of the assessment should be established, including identifying the decisions or actions to which it relates, the decision makers, stakeholders, and the timing and nature of the output required (for example whether qualitative, semi-quantitative or quantitative information is required).

The scope, depth and level of detail of the assessment should be defined, with a description of what is included, and excluded. The types of consequence to be included in the assessment should be defined. Any conditions, assumptions, constraints or necessary resources relevant to the assessment activity should also be specified.

6.1.2 Understand the context

When undertaking a risk assessment those involved should be aware of the broader circumstances in which decisions and actions based on their assessment will be made. This includes understanding the internal and external issues that contribute to the context of the organization as well as wider societal and environmental aspects. Any relevant context statement should be reviewed and checked to see that it is current and appropriate. Understanding the bigger picture is particularly important where there is significant complexity.

6.1.3 Engage with stakeholders

Stakeholders and those who are likely to be able to contribute useful knowledge or relevant views should be identified and their perspectives considered, whether or not they are included as participants in the assessment. Appropriate involvement of stakeholders helps ensure that the information on which risk assessment is based is valid and applicable and that stakeholders understand the reasons behind decisions. Involvement of stakeholders can:

- provide information that enables the context of the assessment to be understood;
- bring together different areas of knowledge and expertise for more effectively identifying and understanding risk;
- provide relevant expertise for use of the techniques;
- enable stakeholder interests to be understood and considered;
- provide input to the process of determining whether risk is acceptable particularly when the stakeholders are impacted;
- fulfil any requirements for people to be informed or consulted;
- obtain support for the outputs and decisions arising from risk assessment;
- identify gaps in knowledge that need to be addressed prior to and/or during risk assessment.

It should be decided how outputs and outcomes of risk assessment are to be reliably, accurately and transparently communicated to relevant stakeholders.

Techniques for eliciting views from stakeholders and experts are described in Clause B.1.

6.1.4 Define objectives

The objectives of the specific system or process for which risk is to be assessed should be defined and where practicable documented. This will facilitate identification of risk and understanding its implications.

To the extent practicable the objectives should be:

- specific to the subject of the assessment;
- measurable either qualitatively or quantitatively;
- achievable within the constraints imposed by the context;
- relevant to the larger goals or context of the organization;
- achievable within a stated time frame.

6.1.5 Consider human, organizational and social factors

Human, organizational and social factors should be considered explicitly and taken into account as appropriate. Human aspects are relevant to risk assessment in the following ways:

- as a source of uncertainty;
- through influences on the way in which techniques are selected and applied;
- in the ways that information is interpreted and used (for example because of differing perceptions of risk).

Human performance (whether above or below expectation) is a source of risk and can also affect the effectiveness of controls. The potential for deviation from expected or assumed behaviours should be specifically considered when assessing risk. Human performance considerations are frequently complex and expert advice can be required to identify and analyse human aspects of risk.

Human factors also influence the selection and use of techniques, particularly where judgements have to be made or team approaches are used. Skilled facilitation is needed to minimize these influences. Biases such as groupthink and over-confidence (for example in estimates or perceptions) should be addressed. Expert opinion should be informed by evidence and data wherever possible and efforts made to avoid or minimize cognitive biases.

People's personal objectives and values can vary and differ from those of the organization. This can result in different perceptions about the level of a risk and different criteria by which individuals make decisions. An organization should endeavour to achieve a common understanding of risk internally and take account of the differing perceptions of stakeholders.

Social aspects, including socioeconomic position, race ethnicity and culture, gender, social relationships and residential and community context can affect risk both directly and indirectly. Impacts may be long term and not immediately visible and can require a long-term planning perspective.

6.1.6 Review criteria for decisions

6.1.6.1 General

Criteria, including risk criteria, which need to be taken into account when making decisions, should be reviewed prior to undertaking the assessment. Criteria can be qualitative, semi-quantitative or quantitative. In some cases there might be no explicit criteria specified and stakeholders use their judgement to respond to the results of analysis.

Relevant criteria to review are:

- how it will be decided whether risk is acceptable;
- how the relative significance of risks will be determined;
- how risk will be taken into account in decisions on options, where each option is associated with multiple risks that might have positive or negative consequences, or both;
- how the relationships between risks will be taken into account.

6.1.6.2 Criteria for deciding whether risk can be accepted

Criteria for defining the nature and extent of risk that can be accepted in pursuit of objectives, sometimes referred to as risk appetite, can be defined by specifying a technique to determine the magnitude of risk, or a parameter related to risk, together with a limit beyond which risk becomes unacceptable. The limit set for unacceptable adverse risk can depend on potential rewards.

The acceptability of risk can also be defined by specifying the acceptable variation in specific performance measures linked to objectives.

Different criteria might be specified according to the type of consequence. For example, an organization's criteria for accepting financial risk may differ from those defined for risk to human life.

The following are examples of considerations used when defining whether risk can be accepted.

- Risk bearing capacity (RBC) (also called risk capacity): An organization's RBC is usually defined in terms of risk capital, which is available for absorbing adverse effects from risks. For a commercial firm capacity might be specified in terms of maximum retention capacity covered by assets, or the largest financial loss the company could bear without having to declare bankruptcy. The estimated RBC should be reasonably tested by stress testing scenarios to provide a reliable confidence level. An organization's risk appetite reflects management's willingness to utilize its RBC.
- ALARP/ALARA and SFAIRP: In some jurisdictions legislated criteria for decisions about treating safety related risk involve ensuring the risk of injury or ill health is "as low as is reasonably practicable" (ALARP), "as low as reasonably achievable" (ALARA) or demonstrating that controls minimize risk "so far as is reasonably practicable" (SFAIRP) (see B.8.2).
- "Globally at least equivalent" (GALE) [*globalement au moins équivalent (GAME)* [1]]: it is considered acceptable for risks with adverse consequences from a particular source to increase if it can be demonstrated that risks from other sources have decreased by an equivalent or greater amount.
- Cost/benefit criteria such as price per life saved or return on investment (ROI).

6.1.6.3 Criteria for evaluating the significance of risk

Risk criteria (the terms of reference against which the significance of risk is determined) can be expressed in terms that involve any of the characteristics and measures of risk elaborated in 6.3.5 and 6.3.7. Ethical, cultural, legal, social, reputational, environmental, contractual, financial and other considerations can also be relevant.

An evaluation of the significance of a risk compared to other risks is often based on an estimate of the magnitude of risk compared with criteria which are directly related to thresholds set around the objectives of the organization. Comparison with these criteria can inform an organization which risks should be focused on for treatment, based on their potential to drive outcomes outside of thresholds set around objectives.

The magnitude of risk is seldom the only criterion relevant to decisions about the significance of risk. Other relevant factors can include sustainability (e.g. triple bottom line) and resilience, ethical and legal criteria, the effectiveness of controls, the maximum impact if controls are not present or fail, the timing of the consequences, the costs of controls and stakeholder views.

Techniques for evaluating the significance of risk are described in Clause B.8

6.1.6.4 Criteria for deciding between options

An organization will be faced with many decisions where several, often competing, objectives are potentially affected, and there are both potential adverse outcomes and potential benefits to consider. For such decisions several criteria might need to be met and trade-offs between competing objectives might be required. Criteria relevant to the decision should be identified and the way in which criteria are to be weighted or trade-offs otherwise made should be decided and accounted for and the information recorded and shared. In setting criteria, the possibility that costs and benefits may differ for different stakeholders should be considered. The way in which different forms of uncertainty are to be taken into account should be decided.

Techniques in Clause B.9 address selecting between options.

6.2 Manage information and develop models

6.2.1 General

Prior to and during a risk assessment, relevant information should be obtained. This information provides an input to statistical analysis, models or to the techniques described in Annexes A and B. In some cases, the information can be used by decision makers without further analysis.

The information needed at each point depends on the results of earlier information gathering, the purpose and scope of the assessment, and the method or methods to be used for analysis. The way information is to be collected, stored, and made available should be decided.

The records of the outputs of the assessment that are to be kept should be decided, along with how those records are to be made, stored, updated and provided to those who might need them. Sources of information should always be indicated.

6.2.2 Collecting information

Information can be gathered from sources such as literature reviews, observations, and expert opinion. Data can be collected or derived, for example, from measurements, experiments, interviews and surveys.

Typically, data directly or indirectly represent past losses or benefits. Examples include project failures or successes, the number of complaints, financial gains or losses, health impacts, injuries and fatalities, etc. Additional information might also be available such as the causes of failures or successes, sources of complaints, the nature of injuries, etc. Data can also include the output from models or other analysis techniques.

The following should be decided:

- the source of information and its reliability;
- type (e.g. whether it is qualitative, quantitative or both (see 6.3.7.1));
- level (e.g. strategic, tactical, operational);
- quantity and quality of the data needed;
- collection methodology;
- level of confidentiality.

When the data to be analysed are obtained from sampling, the statistical confidence that is required should be stated so that sufficient data is collected. Where no statistical analysis is needed this should be stated.

If the data or results from previous assessments are available, it should first be established whether there has been any change in context and, if so, whether the earlier data or results remain relevant.

The validity, reliability and limitations of any information to be used in the assessment should be assessed, taking into account:

- the age and relevance of information;
- the source of information, and the methods used to collect it;
- uncertainties and gaps in the information;
- the authority or provenance of information, data sets, algorithms and models.

6.2.3 Analysing data

Analysis of data can provide:

- an understanding of past consequences and their likelihood in order to learn from experience;
- trends and patterns, including periodicities, that provide an indication of what might influence the future;
- correlations that can give indications of possible causal relationships for further validation.

Limitations and uncertainties in data should be identified and understood.

Past data cannot be assumed to continue to apply into the future, but they can give an indication to decision makers of what is more or less likely to occur in the future.

6.2.4 Developing and applying models

6.2.4.1 General

A model is an approximate representation of reality. Its purpose is to transform what might be an inherently complex situation into simpler terms that can be analysed more easily. It can be used to help understand the meaning of data and to simulate what might happen in practice under different conditions. A model may be physical, represented in software or be a set of mathematical relationships.

Modelling generally includes the following steps:

- describing the problem;
- describing the purpose of building a model and the outcomes desired;
- developing a conceptual model of the problem;
- building a physical, software or mathematical representation of the conceptual model;
- developing software or other tools to analyse how the model behaves;
- processing data;
- validating or calibrating the model by reviewing outputs for known situations;
- drawing conclusions from the model about the real world problem.

Each of these steps can involve approximations, assumptions and expert judgement and (if possible) they should be validated by people independent of the developers. Critical assumptions should be reviewed against available information to assess their credibility.

To achieve reliable results when using models, the following should be validated:

- the conceptual model adequately represents the situation being assessed;
- the model is being used within the contextual limits for which it was designed;
- theoretical concepts underlying the model and any associated calculations are well understood;
- the selection of parameters and mathematical representations of the concepts is sound;
- the mathematics underlying calculations are well understood;
- input data is accurate and reliable, or the nature of the model takes into account the reliability of the input data used;
- the model operates as planned with no internal errors or bugs;
- the model is stable and not overly sensitive to small changes in key inputs.

This can be achieved by:

- performing a sensitivity analysis to check how sensitive the model is to changes in input parameters;

- stress testing the model with particular scenarios, often extreme scenarios;
- comparing outputs with past data (other than those from which it was developed);
- verifying that similar results are obtained when the model is run by different people;
- checking the outputs against actual performance.

Comprehensive documentation of the model and the theories and assumptions on which it is based should be kept, sufficient to enable validation of the model.

6.2.4.2 Using software for analysis

Software programmes can be used to represent and organize data or to analyse it. Software programmes used for modelling and analysis often provide a simple user interface and a rapid output, but these characteristics might lead to invalid results that are unnoticed by the user. Invalid results can arise because of:

- inadequacies in the algorithms used to represent the situation;
- assumptions made in the design and use of the model underlying the software;
- errors in data input including misunderstandings of their meaning;
- data conversion issues when new software is used;
- poor interpretation of outputs.

Commercial software is often black box (commercial in confidence) and might contain any of these errors.

New software should be tested using a simple model with inputs that have a known output, before progressing to test more complex models. The testing details should be retained for use on future version updates or for new software analysis programmes.

Errors in the constructed model can be checked by increasing or decreasing an input value to determine whether the output responds as expected. This can be applied to each of the various inputs. Data input errors are often identified when varying the data inputs. This approach also provides information on the sensitivity of the model to data variations.

A good understanding of the mathematics relevant to the particular analysis is recommended to avoid erroneous conclusions. Not only are the above errors likely, but also the selection of a particular programme might not be appropriate. It is easy to follow a programme and assume that the answer will therefore be right. Evidence should be gathered to check that the outputs are reasonable.

6.3 Apply risk assessment techniques

6.3.1 Overview

The techniques described in Annexes A and B are used to develop an understanding of risk as an input to decisions where there is uncertainty, including decisions about whether and how to treat risk.

Assessment techniques can be used for:

- identifying risk (see 6.3.2);
- determining causes, sources and drivers of risk, and the level of exposure to them (see 6.3.3);
- investigating the overall effectiveness of controls and the modifying effect of proposed risk treatments (see 6.3.4);
- understanding consequences and likelihood (see 6.3.5);

- analysing interactions and dependencies (see 6.3.6);
- providing a measure of risk (see 6.3.7).

Factors to consider when selecting a particular technique for these activities are described in Clause 7.

In general, analysis can be descriptive (such as a report of a literature review, a scenario analysis or a description of consequences) or quantitative, where data are analysed to produce numerical values. In some cases, rating scales can be applied to compare particular risks.

The way in which risk is assessed and the form of the output should be compatible with any defined criteria. For example, quantitative criteria require a quantitative analysis technique which produces an output with the appropriate units.

Mathematical operations should be used only if the chosen metrics allow. In general, mathematical operations should not be used with ordinal scales. Even with fully quantitative analysis, input values are usually estimates. A level of accuracy and precision should not be attributed to results beyond that which is consistent with the data and methods employed.

6.3.2 Identifying risk

Identifying risk enables uncertainty to be explicitly taken into account. All sources of uncertainty and both beneficial and detrimental effects might be relevant, depending on the context and scope of the assessment.

Techniques for identifying risk usually make use of the knowledge and experience of a variety of stakeholders (see B.1.1). They include considering:

- what uncertainty exists and what its effects might be;
- what circumstances or issues (either tangible or intangible) have the potential for future consequences;
- what sources of risk are present or might develop;
- what controls are in place and whether they are effective;
- what, how, when, where, and why events and consequences might occur;
- what has happened in the past and how this might reasonably relate to the future;
- which human aspects and organizational factors might apply.

Physical surveys can also be useful in identifying sources of risk or early warning signs of potential consequences.

The output from risk identification can be recorded as a list of risks with events, causes and consequences specified, or using other suitable formats.

Whatever techniques are used, risk identification should be approached methodically and iteratively so that it is thorough and efficient. Risk should be identified early enough to allow actions to be taken whenever possible. However there are occasions when some risks cannot be identified during a risk assessment. A mechanism should therefore be put in place for capturing emerging risks and recognizing early warning signs of potential success or failure.

Techniques for identifying risk are described in Clause B.2.

6.3.3 Determining sources, causes and drivers of risk

Identifying causes, sources and drivers of risk can:

- contribute towards estimating the likelihood of an event or consequence;

- help to identify treatments that will modify risk;
- assist in determining early warning indicators and their detection thresholds;
- determine common causes which can help develop priorities for treating risk.

Sources of risk can include events, decisions, actions and processes, both favourable and unfavourable, as well as situations that are known to exist but where outcomes are uncertain. Any form of uncertainty described in 4.1 can be a source of risk.

Events and consequences can have multiple causes or causal chains.

Risk can often only be controlled by modifying risk drivers. They influence the status and development of risk exposures, and often affect more than one risk. As a result, risk drivers often need more and closer attention than sources of individual risks.

Techniques for determining sources, causes and drivers of risk are described in Clause B.3.

6.3.4 Investigating the effectiveness of existing controls

Risk is affected by the overall effectiveness of any controls that are in place. The following aspects of controls should be considered:

- the mechanism by which the controls are intended to modify risk;
- whether the controls are in place, are capable of operating as intended, and are achieving the expected results;
- whether there are shortcomings in the design of controls or the way they are applied;
- whether there are gaps in controls;
- whether controls function independently, or if they need to function collectively to be effective;
- whether there are factors, conditions, vulnerabilities or circumstances that can reduce or eliminate control effectiveness including common cause failures;
- whether controls themselves introduce additional risks.

NOTE A risk can have more than one control and controls can affect more than one risk.

A distinction should be made between controls that change likelihood, consequences or both, and controls that change how the burden of risk is shared between stakeholders. For example, insurance and other forms of risk financing do not directly affect the likelihood of an event or its outcomes but can make some of the consequences more tolerable to a particular stakeholder by reducing their extent or smoothing cash flow.

Any assumptions made during risk analysis about the actual effect and reliability of controls should be validated where possible, with a particular emphasis on individual or combinations of controls that are assumed to have a substantial modifying effect. This should take into account information gained through routine monitoring and review of controls.

Techniques for analysing controls are described in Clause B.4

6.3.5 Understanding consequences, and likelihood

6.3.5.1 Analysing the type, magnitude and timing of consequences

Consequence analysis can vary from a description of outcomes to detailed quantitative modelling or vulnerability analysis. Consequential effects (domino or knock-on effects) where one consequence leads to another should be considered where relevant.

Risk can be associated with a number of different types of consequences, impacting different objectives. The types of consequence to be analysed should have been decided when planning the assessment. The context statement should be checked to ensure that the consequences to be analysed align with the purpose of the assessment and the decisions to be made. This can be revisited during the assessment as more is learned.

The magnitude of consequences can be expressed quantitatively as a point value or as a distribution. A distribution can be appropriate where:

- the value for the consequence is uncertain;
- the consequences vary depending on circumstances;
- the parameters that affect consequences vary.

Consideration of the full distribution associated with a consequence provides complete information. It is possible to summarize the distribution in the form of a point value such as the expected value (mean), variation (variance) or the percentage in the tail or some other relevant part of the distribution (percentile).

For any method of obtaining a point value or values to represent a distribution of consequences, there are underlying assumptions and uncertainties about:

- the form of the distribution chosen to fit the data (e.g. continuous or discrete, normal or highly skewed);
- the most appropriate way of representing that distribution as a point value;
- the value of the point estimate because of inherent uncertainties in the data from which the distribution was produced.

It should not be assumed that data relevant to risk necessarily follows a normal distribution.

In some cases information can be summarized as a qualitative or semi-quantitative rating which can be used when comparing risks.

The magnitude of consequences might also vary according to other parameters. For example, the health consequences of exposure to a chemical generally depend on the dose to which the person or other species is exposed. For this example, the risk is usually represented by a dose response curve which depicts the probability of a specified end point (e.g. death) as a function of a short-term or an accumulated dose.

Consequences might also change over time. For example, the adverse impacts of a fault might become more severe the longer the fault exists. Appropriate techniques should be selected to take this into account.

Sometimes consequences result from exposures to multiple sources of risk: for example, environmental or human health effects from the exposure to biological, chemical, physical, and psychosocial sources of risk. In considering multiple exposures the possibility of synergistic effects should be taken into account as well as the influence of the duration and extent of exposure.

6.3.5.2 Analysing likelihood

Likelihood can refer to the likelihood of an event or to the likelihood of a specified consequence. The parameter to which a likelihood value applies should be explicitly stated and the event or consequence whose likelihood is being stated should be clearly and precisely defined. It can be necessary to include a statement about exposure and duration to fully define likelihood.

Likelihood can be described in a variety of ways, including as an expected probability or frequency or in descriptive terms (e.g. "highly likely"). Where a descriptive term is used, its

meaning should be defined. There can be uncertainty in the likelihood which can be shown as a distribution of values representing the degree of belief that a particular value will occur.

Where a percentage is used as a measure of likelihood the nature of the ratio to which the percentage applies should be stated.

EXAMPLE 1 The statement that the chance of a supplier failing to deliver is 5 % is vague in terms of both time period and population. It is also unclear whether the percentage refers to 5 % of projects or 5 % of suppliers. A more explicit statement would be "the probability of one or more suppliers failing to deliver the required goods or services to a project within the life of a project is 5 % of projects".

To minimize misinterpretations when expressing likelihood, either qualitatively or quantitatively, the time period and population concerned should be explicit and consistent with the scope of the particular assessment.

EXAMPLE 2 The probability of one or more suppliers failing to deliver the required goods or services to a project within the next two months is 1 % of projects whereas within a six-month time scale failure can occur in 3 % of projects.

There are many possible biases which can influence estimates of likelihood. Furthermore, interpretation of the likelihood estimate can vary depending on the context within which it is framed. Care should be taken to understand the possible effects of individual (cognitive) and cultural biases.

Techniques for understanding consequences and likelihood are described in Clause B.5.

6.3.6 Analysing interactions and dependencies

There are usually many interactions and dependencies between risks. For example, multiple consequences can arise from a single cause or a particular consequence might have multiple causes. The occurrence of some risks may make the occurrence of others more or less likely, and these causal links can form cascades or loops.

To achieve a more reliable assessment of risk where causal links between risks are significant, it can be useful to create a causal model that incorporates the risks in some form. Common themes can be sought within the risk information such as common causes or drivers of risk, or common outcomes.

Interactions between risks can have a range of impacts on decision making, for example, escalating the importance of activities which span multiple connected risks or increasing the attractiveness of one option over others. Risks might be susceptible to common treatments, or there can be situations such that treating one risk has positive or negative implications elsewhere. Treatment actions can be consolidated at times to significantly reduce the amount of work and more effectively balance available resources. A coordinated treatment plan should take account of these factors rather than assuming that each risk should be treated independently.

Techniques for analysing interactions and dependencies are described in Clause B.6.

6.3.7 Understanding measures of risk

6.3.7.1 Determining measures of risk

In some situations it is useful to provide a measure of risk as some combination of the magnitude of potential consequences and the likelihood of those consequences. This can involve qualitative, semi-quantitative or quantitative measures.

- Qualitative approaches are usually based on descriptive (nominal) or ranking (ordinal) scales for consequences and likelihoods.
- Semi-quantitative approaches include where:

- one parameter (usually likelihood) is expressed quantitatively and the other described or expressed on a rating scale;
- scales are divided into discrete bands, the limits of which are expressed quantitatively. Points on the scale are often set up to have a logarithmic relationship to fit with data;
- numeric descriptors are added to scale points, the meanings of which are described qualitatively.

The use of semi-quantitative scales can lead to misinterpretations if the basis for any calculations is not explained carefully. Therefore, semi-quantitative approaches should be validated and used with caution.

- Quantitative approaches use measures of consequences and likelihoods that are expressed on numerical (ratio) scales. Where a risk is analysed in quantitative terms, it should be ensured that appropriate units and dimensions are used and carried over through the assessment.

Qualitative and semi-quantitative techniques can be used only to compare risks with other risks measured in the same way or with criteria expressed in the same terms. They cannot be used for directly combining or aggregating risks and they are very difficult to use in situations where there are both positive and negative consequences or when trade-offs are to be made between risks.

When quantitative estimates for a consequence and its likelihood are combined as a simple product to provide a magnitude for a risk, information can be lost. In particular, there is no distinction between risks with high consequence and low likelihood and those with low consequences that occur frequently. To compensate for this, a weighting factor may be applied to either the consequence or likelihood; but this should be used with care.

Risk cannot always be adequately described or estimated as a single value representing the likelihood of a specific consequence. Examples where this applies include situations in which:

- consequences are best expressed as a probability distribution of consequences;
- an event has a number of different causes and leads to a range of outcomes and possible consequential effects;
- consequences arise cumulatively from on-going exposure to a source of risk;
- sources of risk (such as systemic problems) are identifiable, but it is very difficult to specify the nature and or likelihood of the consequences that might arise. (In this case estimating a valid magnitude for risk in terms of likelihood and consequence becomes impossible.).

When a risk has a distribution of possible consequences, a measure of risk can be obtained as the probability weighted average of the consequences (i.e. the expectation value). However, this might not always be a good measure of risk because it reflects the mean consequence of the distribution. This results in loss of information about less likely consequences that can be severe and hence important for understanding risk. Techniques for dealing with extreme values are not included in this document.

NOTE An expectation value or expected value is equivalent to summing every consequence/likelihood pair across a distribution, which is equivalent to using the mean consequence of the distribution.

Examples of quantitative metrics of the magnitude of a risk include:

- an expected frequency of occurrence of a specified consequence such as the number of vehicle accidents per thousand kilometres travelled in a region;
- the expected time between events of interest such as the mean up time of an item;
- a probability of a specified end point over a defined period of exposure (relevant when consequences accumulate over a period of exposure) such as the probability of contracting cancer in a life time as a result of exposure to a specified dose of a chemical;

- an expected value, such as the expected returns or financial gains over an investment period, or the expected public health burden in terms of disability adjusted life years per million people per year;
- a statistic representing the shape of a distribution of consequences such as the variance or volatility of returns on an investment;
- a value at or above or below a specified percentile in a consequence distribution;

EXAMPLE The profit from a project that there is a 90 % chance of achieving; or the Value at Risk (VaR) of a portfolio which measures the loss that might arise in a portfolio over a specified time period with a specified probability.

- an extreme measure associated with the distribution of consequences such as the expected maximum consequences.

Consequence based metrics such as the maximum credible loss or probable maximum loss are mainly used when it is difficult to define which controls have the capability of failing or where there is insufficient data on which to base estimates of likelihood.

The magnitude of risk depends on the assumptions made about the presence and effectiveness of relevant controls. Terms such as inherent or gross risk (for the situation where those controls which can fail are assumed to do so) and residual or net risk for the level of a risk when controls are assumed to operate as intended are often used by practitioners. However, it is difficult to define these terms unambiguously and it is therefore advisable to always state explicitly the assumptions made about controls.

When reporting a magnitude of risk, either qualitatively or quantitatively, the uncertainties associated with assumptions and with the input and output parameters should be described.

6.3.7.2 Aggregating measures of risk

In some cases (such as for capital allocation) it can be useful to combine values for a set of risks to produce a single value. Provided the risks are characterized by a single consequence, measured in the same units, such as monetary value, they can in principle be combined. That is, they can be combined only when consequences and likelihood are stated quantitatively and the units are consistent and correct. In some situations, a measure of utility can be used as a common scale to quantify and combine consequences that are measured in different units.

Developing a single consolidated value for a set of more complex risks loses information about the component risks. In addition, unless great care is taken, the consolidated value can be inaccurate and has the potential to be misleading. All methods of aggregating risks to a single value have underlying assumptions which should be understood before being applied. Data should be analysed to seek correlations and dependencies which will affect how risks combine. Modelling techniques used to produce an aggregate level of risk should be supported by scenario analysis and stress testing.

Where models incorporate calculations involving distributions, they should include correlations between those distributions in an appropriate manner. If correlation is not taken into account appropriately the outcomes will be inaccurate and may be grossly misleading. Consolidating risks by simply adding them up is not a reliable basis for decision making and could lead to undesired results. Monte Carlo simulation can be used to combine distributions (see B.5.10).

Qualitative or semi-quantitative measures of risk cannot be directly aggregated. Equally, only general qualitative statements can be made about the relative effectiveness of controls based on qualitative or semi-quantitative measures of changes in level of risk.

Relevant data about different risks can be brought together in a variety of ways to assist decision makers. It is possible to conduct a qualitative aggregation based on expert opinion, taking into account more detailed risk information. The assumptions made and information used to conduct qualitative aggregations of risk should be clearly articulated.

6.3.7.3 Societal risk

Where a population is exposed to risk, a simple aggregation of the individual level of risk by multiplying by the population exposed, in most cases, does not adequately represent the true impact of the consequences. For example, an individual's risk of a fatality from an event such as a dam failure might need to be considered differently from the same event affecting a group of individuals together.

Societal risk is typically expressed and evaluated in terms of the relationship between the frequency of occurrence of a consequence (F) and the number of people bearing the consequences (N). (See F-N diagrams in B.8.3).

Techniques that provide a measure of risk are described in Clause B.7.

6.4 Review the analysis

6.4.1 Verifying and validating results

Where practicable, results of analysis should be verified and validated. Verification involves checking that the analysis was done correctly. Validation involves checking that the right analysis was done to achieve the required objectives. For some situations verification and validation can involve independent review processes.

Validation can include:

- checking that the scope of the analysis is appropriate for the stated goals;
- reviewing all critical assumptions to ensure they are credible in the light of available information;
- checking that appropriate methods, models and data were used;
- using multiple methods, approximations and sensitivity analysis to test and validate conclusions.

Verification can include:

- checking the validity of mathematical manipulations and calculations;
- checking that the results are insensitive to the way data or results are displayed or presented;
- comparing results with past experience where data exists or by comparison with outcomes after they occur;
- establishing whether the results are sensitive to the way data or results are displayed or presented and to identify input parameters that have a significant effect on the results of the assessment;
- comparing results with past or subsequent experience including explicitly obtaining feedback as time progresses.

6.4.2 Uncertainty and sensitivity analysis

Those analysing risk should understand the uncertainties in the analysis and appreciate the implications for the reliability of the results. Uncertainties and their implications should always be communicated to decision makers.

Uncertainty in analysis outputs can arise because:

- there is variability in the system being considered;
- the data is from an unreliable source, inconsistent or insufficient – for example, the type of data collected or methods of collection might have changed;

- there might be ambiguity, for example in the way that qualitative descriptors are stated or understood;
- the analysis method does not adequately represent the complexity of the system;
- there is a high reliance on people's expert opinion or judgement;
- relevant data might not exist or the organization might not have collected the data needed;
- data from the past might not provide a reliable basis from which to forecast the future because something within the context or circumstances has changed;
- there are uncertainties or approximations in the assumptions that are made.

When a lack of reliable data is recognized during the analysis, further data should be collected, if practicable. This can involve implementing new monitoring arrangements. Alternatively, the analysis process should be adjusted to take account of the data limitations.

A sensitivity analysis can be carried out to evaluate the significance of uncertainties in data or in the assumptions underlying the analysis. Sensitivity analysis involves determining the relative change to the results brought about by changes in individual input parameters. It is used to identify data that need to be accurate, and those that are less sensitive and hence have less effect upon overall accuracy. Parameters to which the analysis is sensitive and the degree of sensitivity should be stated where appropriate.

Parameters that are critical to the assessment and that are subject to change should be identified for on-going monitoring, so that the risk assessment can be updated, and, if necessary, decisions reconsidered.

6.4.3 Monitoring and review

Monitoring can be used:

- to compare actual outcomes with the results predicted by risk assessment and hence improve future assessments;
- to look for precursors and early indicators of potential consequences that were identified by the assessment;
- to collect data needed for a good understanding of risk;
- to scan for new risk and unexpected changes that can indicate a need to update assessment.

Where a sensitivity analysis indicates parameters of particular importance to the outcome of an analysis, these should also be considered for monitoring.

Assessments should be reviewed periodically to identify whether change has occurred, including changes in the context or in assumptions, and whether there is new information or new methods available.

6.5 Apply results to support decisions

6.5.1 Overview

The outcomes from risk analysis provide an input to decisions that need to be made and actions that are taken.

NOTE An understanding of risk can inform actions even where no explicit decision-making process is followed.

The factors to consider when making decisions and any specific criteria should have been defined as part of establishing the context for the assessment (see 6.1.6).

Two types of decisions can be distinguished:

- decisions about the significance of risk and whether and how to treat risk;
- decisions that involve comparing options where each has uncertainties (such as which of several opportunities to pursue).

6.5.2 Decisions about the significance of risk

The information from risk identification and analysis can be used to draw conclusions about whether the risk should be accepted and the comparative significance of the risk relative to the objectives and performance thresholds of the organization. This provides an input into decisions about whether risk is acceptable or requires treatment, and any priorities for treatment.

Some risks may be accepted for a finite time (for example, to allow time to actually implement treatments). The assessor should be clear about the mechanisms for temporarily accepting risks and the process to be used for subsequent reconsideration.

Priorities for treatment, for monitoring or for more detailed analysis are often based on a magnitude of risk obtained by combining a representative consequence and its likelihood, and displayed using a consequence/likelihood matrix (B.10.3). This method has some limitations (see B.10.3.5 and 6.3.7.1). Factors other than the magnitude of risk that can be taken into account in deciding priorities include:

- other measures associated with the risk such as the maximum or expected consequences or the effectiveness of controls;
- the qualitative characteristics of events or their possible consequences;
- the views and perceptions of stakeholders;
- the cost and practicability of further treatment compared with the improvement gained;
- interactions between risks including the effects of treatments on other risks.

Once risks have been evaluated and treatments decided, the risk assessment process can be repeated to check that proposed treatments have not created additional adverse risks and that the risk remaining after treatment is within the organization's risk appetite.

Techniques for evaluating the significance of risk are described in Clause B.8.

6.5.3 Decisions that involve selecting between options

Selecting between options normally involves weighing the potential advantages and disadvantages of each option taking into account uncertainties including:

- uncertainties associated with the potential outcomes of the options and estimates of costs and benefits;
- potential events and developments that may affect outcomes;
- the varied values that different stakeholders place on costs and benefits;
- uncertainty around judgements made from the outputs of risk analysis, including considerations such as whether objectives and criteria will continue unchanged into the future.

This type of decision is often made using expert judgement based on the understanding from an analysis of the options concerned and the risk associated with each, taking into account:

- trade-offs that may need to be made between competing objectives;
- the organization's appetite for risk;
- the different attitudes and beliefs of stakeholders.

Techniques that can be used when comparing options that involve uncertainty are described in Clause B.9.

6.6 Record and report risk assessment process and outcomes

The results of risk assessment, the methodologies used and the rationale for assumptions and any recommendations should be documented and a decision made about what information needs to be communicated and to whom. The way in which records are to be reviewed and updated should be defined.

The purpose of records is to:

- communicate information about risk to decision makers and other stakeholders including regulators;
- provide a record and justification of the rationale for decisions made;
- preserve the results of assessment for future use and reference;
- track performance and trends;
- provide confidence that risks are understood and are being managed appropriately;
- enable verification of the assessment;
- provide an audit trail.

It follows that any documentation or records should be provided in a timely manner and be in a form that can be understood by those who will read it. Documents should also provide the necessary technical depth for validation, and sufficient detail to preserve the assessment for future use. The information provided should be sufficient to allow both the processes followed and the outcomes to be reviewed and validated. Assumptions made, limitations in data or methods, and reasons for any recommendations made should be clear.

Risk should be expressed in understandable terms, and the units in which quantitative measures are expressed should be clear and correct.

Those presenting the results should characterize their confidence or that of their team in the accuracy and completeness of the results. Uncertainties should be adequately communicated so that the report does not imply a level of certainty beyond the reality.

Techniques for recording and reporting are described in Clause B.10.

7 Selecting risk assessment techniques

7.1 General

Clause 7 describes factors to consider when selecting a technique or techniques for a particular purpose. Annexes A and B list and further explain some commonly used techniques. They describe the characteristics of each technique and its possible range of application, together with its inherent strengths and weaknesses.

Many of the techniques described in this document were originally developed for particular industries seeking to manage particular types of unwanted outcomes. Several of the techniques are similar, but use different terminologies, reflecting their independent development for a similar purpose in different sectors. Over time the application of many of the techniques has broadened, for example extending from technical engineering applications to financial or managerial situations, or to consider positive as well as negative outcomes. New techniques have emerged and old ones have been adapted to new circumstances. The techniques and their applications continue to evolve. There is potential for enhanced understanding of risk by using techniques outside their original application. Annexes A and B therefore indicate the characteristics of techniques that can be used to determine the range of circumstances to which they can be applied.

7.2 Selecting techniques

The choice of technique and the way it is applied should be tailored to the context and use, and provide information of the type and form needed by the stakeholders. In general terms, the number and type of technique selected should be scaled to the significance of the decision, and take into account constraints on time and other resources, and opportunity costs.

In deciding whether a qualitative or quantitative technique is more appropriate, the main criteria to consider are the form of output of most use to stakeholders and the availability and reliability of data. Quantitative techniques generally require high quality data if they are to provide meaningful results. However, in some cases where data is not sufficient, the rigour needed to apply a quantitative technique can provide an improved understanding of the risk, even though the result of the calculation might be uncertain.

There is often a choice of techniques relevant for a given circumstance. Several techniques might need to be considered, and applying more than one technique can sometimes provide useful additional understanding. [2] Different techniques can also be appropriate as more information becomes available.

In selecting a technique or techniques the following should therefore be considered:

- the purpose of the assessment;
- the needs of stakeholders;
- any legal, regulatory and contractual requirements;
- the operating environment and scenario;
- the importance of the decision (e.g. the consequences if a wrong decision is made);
- any defined decision criteria and their form;
- the time available before a decision must be made;
- information that is available or can be obtained;
- the complexity of the situation;
- the expertise available or that can be obtained.

The characteristics of the techniques relevant to these requirements are listed in Table A.1. Table A.2 provides a list of techniques, classified according to these characteristics.

As the degree of uncertainty, complexity and ambiguity of the context increases then the need to consult a wider group of stakeholders will increase, with implications for the combination of techniques selected.

NOTE For example, IEC TR 63039:2016 [50] guides how to use ETA, FTA and Markov techniques in a complementary way so that the combined use is an efficient way to analyse risk of complex systems.

Some of the techniques described in this document can be applied during steps of the ISO 31000 risk management process in addition to their usage in risk assessment. Application of the techniques to the risk management process is illustrated in Figure A.1. Table A.3 illustrates their application specifically to assessment.

Annex B contains an overview of each technique, its use, its inputs and outputs, its strengths and limitations and, where applicable, a reference for where further detail can be found. It categorizes techniques according to their primary application in assessing risk, namely:

- eliciting views from stakeholders and experts, (Clause B.1);
- identifying risk (Clause B.2);
- determining sources, causes and drivers of risk (Clause B.3);
- analysing existing controls (Clause B.4);

- understanding consequences and likelihood (Clause B.5);
- analysing dependencies and interactions (Clause B.6);
- providing measures of risk (Clause B.7);
- evaluating the significance of risk (Clause B.8);
- selecting between options (Clause B.9);
- recording and reporting (Clause B.10).

Within each grouping, techniques are arranged alphabetically and no order of importance is implied.

The majority of techniques in Annex B assume that risks or sources of risk can be identified. There are also techniques which can be used to indirectly assess residual risk by considering controls and requirements that are in place (see for example IEC 61508 [36]).

While this document discusses and provides example techniques, the techniques described are non-exhaustive and no recommendation is made as to the efficacy of any given technique in any given circumstance. Care should be taken in selecting any technique to ensure that it is appropriate, reliable and effective in the given circumstance.

Annex A (informative)

Categorization of techniques

A.1 Introduction to categorization of techniques

Table A.1 explains the characteristics of techniques that can be used for selecting which technique or techniques to use.

Table A.1 – Characteristics of techniques

Characteristic	Description	Details (e.g. features indicators)
Application	How the technique is used in risk assessment (see titles of Clauses B.1 to B.10)	Elicit views, identify, analyse cause, analyse controls, etc.
Scope	Applies to risk at organizational level, departmental or project level or individual processes or equipment level	organization (org) project/department (dep) equipment/process (equip/proc)
Time horizon	Looks at short-, medium- or long-term risk or is applicable to any time horizon	Short, medium, long, any
Decision level	Applies to risk at a strategic, tactical or operational level	Strategic (1), tactical (2), operational (3)
Starting info/data needs	The level of starting information or data needed	High, medium, low
Specialist expertise	Level of expertise required for correct use	low: intuitive or one to two days' training moderate: training course of more than two days high: requires significant training or specialist expertise
Qualitative – quantitative	Whether the method is qualitative, semi-quantitative or quantitative	quantitative (quant) qualitative (qual) semi-quantitative (semi-quant) can be used qualitatively or quantitatively (either)
Effort to apply	Time and cost required to apply technique	high, medium, low

A.2 Application of categorization of techniques

Table A.2 lists a range of techniques classified according to these characteristics. The techniques described represent structured ways of looking at the problem in hand that have been found useful in particular contexts. The list is not intended to be comprehensive but covers a range of commonly used techniques from a variety of sectors. For simplicity the techniques are listed in alphabetical order without any priority.

Each technique is described in more detail in Annex B, as referenced in column 1 of Table A.2.

Table A.2 – Techniques and indicative characteristics

Sub-clause	Technique	Description	Application	Scope	Time horizon	Decision level	Starting info/data needs	Specialist expertise	Qual/quant/semi-quant	Effort to apply
B.8.2	ALARP/SFAIRP	Criteria for deciding significance of risk and means of evaluating tolerability of risk.	evaluate risk	1	any	1/2	high	high	qual/quant	high
B.5.2	Bayesian analysis	A means of making inference about model parameters using Bayes' theorem which has the capability of incorporating empirical data into prior judgements about probabilities.	analyse likelihood	any	any	any	medium	high	quant	medium
B.5.3	Bayesian networks/ Influence diagrams	A graphical model of variables and their cause-effect relationships expressed using probabilities. A basic Bayesian network has variables representing uncertainties. An extended version, known as an influence diagram, includes variables representing uncertainties, consequences and actions.	identify risk estimate risk decide between options	any	any	any	medium	high	quant	medium/ high
B.4.2	Bow tie analysis	A diagrammatic way of describing the pathways from sources of risk to outcomes, and of reviewing controls.	Analyse risk analyse controls describe risk	2/3	short/ medium	any	low	low/ moderate	qual/semi-quant	low
B.1.2	Brainstorming	Technique used in workshops to encourage imaginative thinking.	elicit views	any	any	any	none	low/ moderate	qual	low
B.5.4	Business impact analysis	The BIA process analyses the consequences of a disruptive incident on the organization which determines the recovery priorities of an organization's products and services and, thereby, the priorities of the activities and resources which deliver them.	analyse conseq. analyse controls	1	short/ medium	2	medium	low	quant/qual	medium
B.6.1	Causal mapping	A network diagram representing events, causes and effects and their relationships.	analyse causes	2/3	any	2/3	medium	moderate	qual	medium
B.5.5	Cause-consequence analysis	A combination of fault and event tree analysis that allows inclusion of time delays. Both causes and consequences of an initiating event are considered.	analyse causes and conseq.	2/3	any	2/3	medium/ high	moderate/ high	quant	medium/ high

Sub-clause	Technique	Description	Application	Scope	Time horizon	Decision level	Starting info/data needs	Specialist expertise	Qual/quant/semi-quant	Effort to apply
B.2.2	Checklists classifications, taxonomies	Lists based on experience or on concepts and models that can be used to help identify risks or controls.	identify risk or controls	2/3	any	any	high to develop, low to use	low/moderate	qual	low/medium
B.3.2	Cindynic approach	Considers goals, values, rules, data and models of stakeholders and identifies inconsistencies, ambiguities, omissions and ignorance. These form systemic sources and drivers of risk.	identify risk drivers	1/2	short or medium	1	low	moderate	qual	high
B.7.3	Conditional value at risk CVaR	Also called expected shortfall (ES), is a measure of the expected loss from a financial portfolio in the worst a % of cases.	measure of risk	any	short/medium	3	high	high	quant	medium
B.10.3	Consequence/likelihood matrix	Compares individual risks by selecting a consequence/likelihood pair and displaying them on a matrix with consequence on one axis and likelihood on the other.	report risks evaluate	any	any	any	medium	low to use, moderate to develop	qual/semi-quant/quant	low
B.9.2	Cost/benefit analysis	Uses money as a scale for estimating positive and negative, tangible and intangible, consequences of different options.	compare options	any	short/medium	any	medium/high	moderate/high	quant	medium/high
B.6.2	Cross impact analysis	Evaluates changes in the probability of the occurrence of a given set of events consequent on the actual occurrence of one of them.	analyse likelihood and cause	any	short/medium	any	low to high	moderate/high	quant	medium/high
B.9.3	Decision tree analysis	Uses a tree-like representation or model of decisions and their possible consequences. Outcomes are usually expressed in monetary terms or in terms of utility. An alternative representation of a decision tree is an influence diagram (see B.5.3).	compare options	any	any	2	low/ medium	moderate	quant	medium
B.1.3	Delphi technique	Collects judgements through a set of sequential questionnaires. People participate individually but receive feedback on the responses of others after each set of questions.	elicit views	any	any	any	none	moderate	qual	medium

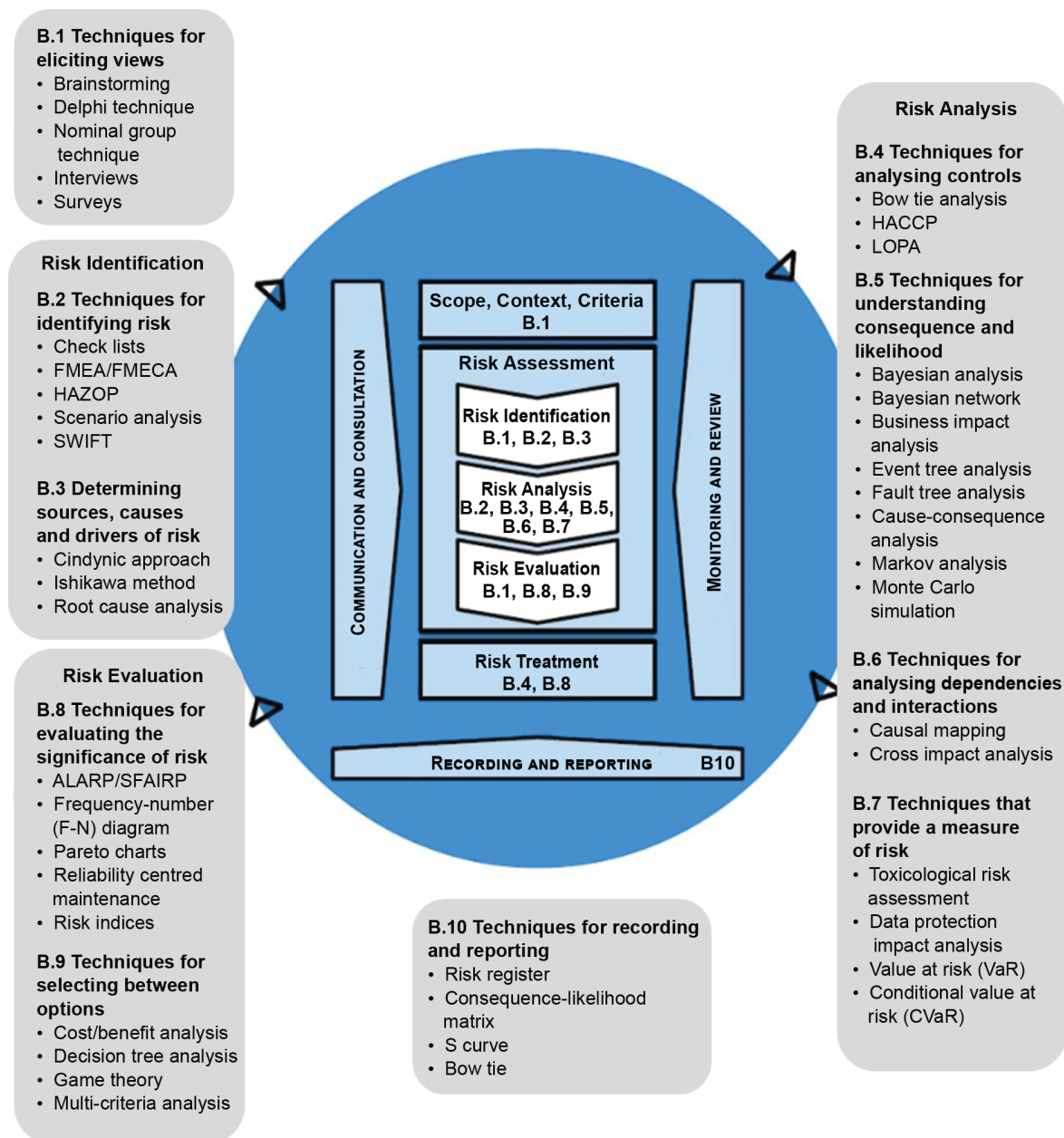
Sub-clause	Technique	Description	Application	Scope	Time horizon	Decision level	Starting info/data needs	Specialist expertise	Qual/quant/semi-quant	Effort to apply
B.5.6	Event tree analysis (ETA)	Models the possible outcomes from a given initiating event and the status of controls thus analysing the frequency or probability of the various possible outcomes.	analyse conseq. and controls	2/3	any	any	low/medium	moderate	qual/quant	medium
B.5.7	Fault tree analysis (FTA)	Analyses causes of a focus event using Boolean logic to describe combinations of faults. Variations include a success tree where the top event is desired and a cause tree used to investigate past events.	analyse likelihood analyse causes	2/3	medium	2/3	high for quant analysis	depends on complexity	qual/quant	medium/ high
B.2.3	Failure modes and effects (and criticality) analysis FME(C)A	Considers the ways in which each component of a system might fail and the failure causes and effects. FMEA can be followed by a criticality analysis which defines the significance of each failure mode (FMECA).	identify risks	2/3	any	2/3	depends on application	moderate	qual/semi- quant/quant	low /high
B.8.3	Frequency / number (F/N) diagrams	Special case of quantitative consequence/likelihood graph applied to consideration of tolerability of risk to human life.	evaluate risk	1	any	any	high	high	quant	high
B.9.4	Game theory	The study of strategic decision making to model the impact of the decisions of different players involved in the game. Example application area can be risk based pricing.	decide between options	1	medium	1/2	high	high	quant	medium/ high
B.4.3	Hazard analysis and critical control points (HACCP)	Analyses the risk reduction that can be achieved by various layers of protection.	analyse controls monitor	2/3	short/ medium	2/3	medium	moderate	qual	medium
B.2.4	Hazard and operability studies (HAZOP)	A structured and systematic examination of a planned or existing process or operation in order to identify and evaluate problems that might represent risk to personnel or equipment, or prevent efficient operation.	identify and analyse risks	3	medium/ long	2/3	medium	facilitator: high, participants: moderate	qual	medium/ high
B.5.8	Human reliability analysis (HRA)	A set of techniques for identifying the potential for human error and estimating the likelihood of failure.	analyse risk and sources of risk	2/3	any	2/3	medium	high	qual/quant	medium to high
B.1.5	Interviews	Structured or semi- structured one-to-one conversations to elicit views.	elicit views	any	any	any	none	moderate	qual	high

Sub-clause	Technique	Description	Application	Scope	Time horizon	Decision level	Starting info/data needs	Specialist expertise	Qual/quant/semi-quant	Effort to apply
B.3.3	Ishikawa analysis (fishbone diagram)	Identifies contributory factors to a defined outcome (wanted or unwanted). Contributory factors are usually divided into predefined categories and displayed in a tree structure or a fishbone diagram.	analyse sources of risk	any	any	any	low	low/moderate	qual	low
B.4.4	Layers of protection analysis (LOPA)	Analyses the risk reduction that can be achieved by various layers of protection.	analyse controls	3	any	2/3	medium	moderate/high	qual/quant	medium/high
B.5.9	Markov analysis	Calculates the probability that a system that has the capacity to be in one of a number of states will be in a particular state at a time t in the future.	analyse likelihood	3	any	2/3	medium/high	high	quant	medium
B.5.10	Monte Carlo analysis	Calculates the probability of outcomes by running multiple simulations using random variables.	analyse likelihood	any	any	any	medium	high	quant	medium/high
B.9.5	Multi-criteria analysis (MCA)	Compares options in a way that makes trade-offs explicit. Provides an alternative to cost/benefit analysis that does not need a monetary value to be allocated to all inputs.	decide between options	any	any	any	low	moderate	qual	low/medium
B.1.4	Nominal group technique	Technique for eliciting views from a group of people where initial participation is as individuals with no interaction, then group discussion of ideas follows.	elicit views	any	any	any	none	low	qual	medium
B.8.4	Pareto charts	The Pareto principle (the 80–20 rule) states that, for many events, roughly 80 % of the effects come from 20 % of the causes.	set priorities	any	any	any	medium	moderate	semi-quant/quant	low
B.5.11	(PIA/DPIA) privacy impact analysis / data protection impact analysis	Analyses how incidents and events could affect a person's privacy (PI) and identifies and quantifies the capabilities that would be needed to manage it.	analyse sources of risk conseq analysis	any	any	1/2	medium	moderate/high	qual	medium
B.8.5	Reliability centred maintenance (RCM)	A risk based assessment used to identify the appropriate maintenance tasks for a system and its components.	evaluate risk decide controls	2/3	medium	2/3	medium	high for facilitator, moderate to use	qual/semi-quant/quant	medium/high

Sub-clause	Technique	Description	Application	Scope	Time horizon	Decision level	Starting info/data needs	Specialist expertise	Qual/quant/semi-quant	Effort to apply
B.8.6	Risk indices	Rates the significance of risks based on ratings applied to factors which are believed to influence the magnitude of the risk.	compare risks	any	any	any	medium	low to use, moderate to develop	semi-quant	low
B.10.2	Risk registers	A means of recording information about risks and tracking actions.	recording and reporting risks monitor and review	any	any	any	low/medium	low/moderate	qual	medium
B.10.4	S-curves	A means of displaying the relationship between consequences and their likelihood plotted as a cumulative distribution function (S-curve).	display risk evaluate risk	any	any	2/3	medium/high	moderate/high	quant/semi-quant	medium
B.2.5	Scenario analysis	Identifies possible future scenarios through imagination, extrapolation from the present or modelling. Risk is then considered for each of these scenarios.	identify risk, conseq. analysis	any	medium or long	any	low/medium	moderate	qual	low/medium
B.1.6	Surveys	Paper- or computer-based questionnaires to elicit views.	elicit views	any	medium/long	2/3	low	moderate	qual	high
B.2.6	Structured what if technique (SWIFT)	A simpler form of HAZOP with prompts of "what if" to identify deviations from the expected.	identify risk	1/2	medium/long	1/2	medium	low/moderate	qual	low/medium
B.7.1	Toxicological risk assessment	A series of steps taken to obtain a measure for the risk to humans or ecological systems due to exposure to chemicals.	measure of risk	3	medium/long	2/3	high	high	quant	high
B.7.2	Value at risk (VaR)	Financial measure of risk that uses an assumed probability distribution of losses in a stable market condition to calculate the value of a loss that might occur with a specified probability within a defined time span.	measure of risk	any	short/medium	3	high	high	quant	medium

A.3 Use of techniques during the ISO 31000 process

Table A.3 lists the extent to which each technique is applicable to the different stages of risk assessment; namely risk identification, risk analysis, and risk evaluation. Some of the techniques are also used in other steps of the process. This is illustrated in Figure A.1.



IEC

Figure A.1 – Application of techniques in the ISO 31000 risk management process [3]

NOTE Figure A.1 is intended to provide an overview and is not an exhaustive list of all techniques that can be used at each step.

Table A.3 – Applicability of techniques to the ISO 31000 process

Tools and techniques	Risk assessment process					Sub-clause
	Risk identification	Risk analysis			Risk evaluation	
		Consequence	Likelihood	Level of risk		
ALARP, ALARA and SFAIRP	NA	NA	NA	NA	SA	B.8.2
Bayesian analysis	NA	NA	SA	NA	NA	B.5.2
Bayesian networks	NA	NA	SA	NA	SA	B.5.3
Bow tie analysis	A	SA	A	A	A	B.4.2
Brainstorming	SA	A	NA	NA	NA	B.1.2
Business impact analysis	A	SA	NA	NA	NA	B.5.4
Causal mapping	A	A	NA	NA	NA	B.6.1
Cause-consequence analysis	A	SA	SA	A	A	B.5.5
Checklists, classifications and taxonomies	SA	NA	NA	NA	NA	B.2.2
Cindynic approach	SA	NA	NA	NA	NA	B.3.2
Consequence/likelihood matrix	NA	A	A	SA	A	B.10.3
Cost/benefit analysis	NA	SA	NA	NA	SA	B.9.2
Cross impact analysis	NA	NA	SA	NA	NA	B.6.2
Decision tree analysis	NA	SA	SA	A	A	B.9.3
Delphi technique	SA	NA	NA	NA	NA	B.1.3
Event tree analysis	NA	SA	A	A	A	B.5.6
Failure modes and effects analysis	SA	SA	NA	NA	NA	B.2.3
Failure modes and effects and criticality analysis	SA	SA	SA	SA	SA	B.2.3
Fault tree analysis	A	NA	SA	A	A	B.5.7
F-N diagrams	A	SA	SA	A	SA	B.8.3
Game theory	A	SA	NA	NA	SA	B.9.4
Hazard and operability studies (HAZOP)	SA	A	NA	NA	NA	B.2.4
Hazard analysis and critical control points (HACCP)	SA	SA	NA	NA	SA	B.4.3
Human reliability analysis	SA	SA	SA	SA	A	B.5.8
Ishikawa (fishbone)	SA	A	NA	NA	NA	B.3.3
Layer protection analysis (LOPA)	A	SA	A	A	NA	B.4.4
Markov analysis	A	A	SA	NA	NA	B.5.9
Monte Carlo simulation	NA	A	A	A	SA	B.5.10
Multi-criteria analysis (MCA)	A	NA	NA	NA	SA	B.9.5
Nominal group technique	SA	A	A	NA	NA	B.1.4
Pareto charts	NA	A	A	A	SA	B.8.4
Privacy impact analysis/ data privacy impact assessment (PIA/DPIA)	A	SA	A	A	SA	B.5.11
Reliability centred maintenance	A	A	A	A	SA	B.8.5
Risk indices	NA	SA	SA	A	SA	B.8.6
S-curves	NA	A	A	SA	SA	B.10.4
Scenario analysis	SA	SA	A	A	A	B.2.5

Tools and techniques	Risk assessment process					Sub-clause
	Risk identification	Risk analysis			Risk evaluation	
		Consequence	Likelihood	Level of risk		
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B.1.5
Structured "What if?" (SWIFT)	SA	SA	A	A	A	B.2.6
Surveys	SA	NA	NA	NA	NA	B.1.6
Toxicological risk assessment	SA	SA	SA	SA	SA	B.7.1
Value at risk (VaR)	NA	A	A	SA	SA	B.7.2
A: applicable; SA: strongly applicable; NA: not applicable.						

Annex B (informative)

Description of techniques

B.1 Techniques for eliciting views from stakeholders and experts

B.1.1 General

Some of the techniques described in Clauses B.2 to B.7 involve input from stakeholders and experts. This provides for a breadth of expertise and allows stakeholder involvement. Stakeholder and expert views can be obtained on an individual basis (e.g. through interview or survey) or using group techniques such as brainstorming, nominal groups or Delphi technique. Views can include disclosure of information, expressions of opinion or creative ideas. Clause B.1 describes some techniques that can be used to elicit information or gain consensus.

In some situations stakeholders have a specific expertise and role, and there is little divergence of opinion. However, sometimes significantly varying stakeholder views might be expected and there might be power structures and other factors operating that affect how people interact. These factors will affect the choice of method used. The number of stakeholders to be consulted, time constraints and the practicalities of getting all necessary people together at the same time will also influence the choice of method.

Where a group face-to-face method is used, an experienced and skilled facilitator is important to achieving good outputs. The role of the facilitator or coordinator is to:

- organize the team;
- obtain and distribute relevant information and data prior to the meeting/collaboration;
- prepare an efficient structure and format for the meeting/collaboration;
- provoke creative thinking in order to strengthen understanding and to generate ideas;
- ensure the results are accurate and as free from bias as possible.

Checklists derived from classifications and taxonomies can be used as part of the process (see B.2.2).

Any technique for obtaining information that relies on people's perceptions and opinions has the potential to be unreliable and suffers from a variety of biases such as availability bias (a tendency to over-estimate the likelihood of something which has just happened), clustering illusion (the tendency to overestimate the importance of small clusters in a large sample) or bandwagon effect (the tendency to do or believe things because others do or believe the same).

Guidance on function analysis which can be used to reduce bias and focus creative thinking on aspects which have the greatest impact is given in EN 12973 [4].

The information on which judgements were based and any assumptions made should be reported.

B.1.2 Brainstorming

B.1.2.1 Overview

Brainstorming is a process used to stimulate and encourage a group of people to develop ideas related to one of more topics of any nature. The term "brainstorming" is often used very loosely to mean any type of group discussion, but effective brainstorming requires a conscious effort to ensure that the thoughts of others in the group are used as tools to stimulate the creativity

of each participant. Any analysis or critique of the ideas is carried out separately from the brainstorming.

This technique gives the best results when an expert facilitator is available who can provide necessary stimulation but does not limit thinking. The facilitator stimulates the group to cover all relevant areas and makes sure that ideas from the process are captured for subsequent analysis.

Brainstorming can be structured or unstructured. For structured brainstorming the facilitator breaks down the issue to be discussed into sections and uses prepared prompts to generate ideas on a new topic when one is exhausted. Unstructured brainstorming is often less formal. In both cases the facilitator starts off a train of thought and everyone is expected to generate ideas. The pace is kept up to allow ideas to trigger lateral thinking. The facilitator can suggest a new direction, or apply a different creative thinking tool when one direction of thought is exhausted or discussion deviates too far. The goal is to collect as many diverse ideas as possible for later analysis.

It has been demonstrated that, in practice, groups generate fewer ideas than the same people working individually. For example:

- in a group, people's ideas tend to converge rather than diversify;
- the delay in waiting for a turn to speak tends to block ideas;
- people tend to work less hard mentally when in a group.

These tendencies can be reduced by:

- providing opportunities for people to work alone for part of the time;
- diversifying teams and changing team membership;
- combining with techniques such as nominal group technique (B.1.4) or electronic brainstorming. These encourage more individual participation and can be set up to be anonymous, thus also avoiding personal political and cultural issues.

B.1.2.2 Use

Brainstorming can be applied at any level in an organization to identify uncertainties, success or failure modes, causes, consequences, criteria for decisions or options for treatment. Quantitative use is possible but only in its structured form to ensure that biases are taken into account and addressed, especially when used to involve all stakeholders.

Brainstorming stimulates creativity and is therefore very useful when working on innovative designs, products and processes.

B.1.2.3 Inputs

Brainstorming elicits views from participants so has less need for data or external information than other methods. Participants need to have between them the expertise, experience and range of viewpoints needed for the problem in hand. A skilled facilitator is normally necessary for brainstorming to be productive.

B.1.2.4 Outputs

The outputs are a list of all the ideas generated during the session and the thoughts raised when the ideas were presented.

B.1.2.5 Strengths and limitations

Strengths of brainstorming include the following.

- It encourages imagination and creativity, which helps identify new risks and novel solutions.

- It is useful where there is little or no data, and where new technology or novel solutions are required.
- It involves key stakeholders and hence aids communication and engagement.
- It is relatively quick and easy to set up.

Limitations include the following.

- It is difficult to demonstrate that the process has been comprehensive.
- Groups tend to generate fewer ideas than the individuals working alone.
- Particular group dynamics might mean some people with valuable ideas stay quiet while others dominate the discussion. This can be overcome by effective facilitation.
- Encouraging creative thinking and new ideas can mean that conversation does not stay focused on the matter being considered, and this takes up meeting time.

B.1.2.6 Reference documents

[5] PROCTOR, A. (2009). *Creative problem solving for managers*

[6] GOLDENBERG, Olga, WILEY, Jennifer. *Quality, conformity, and conflict: Questioning the assumptions of Osborn's brainstorming technique*

B.1.3 Delphi technique

B.1.3.1 Overview

The Delphi technique is a procedure to gain consensus of opinion from a group of experts. It is a method to collect and collate judgments on a particular topic through a set of sequential questionnaires. An essential feature of the Delphi technique is that experts express their opinions individually, independently and anonymously while having access to the other experts' views as the process progresses.

The group of experts who form the panel are independently provided with the question or questions to be considered. The information from the first round of responses is analysed and combined and circulated to panellists who are then able to reconsider their original responses. Panellists respond and the process is repeated until consensus or quasi consensus is reached. If one panellist or a minority of panellists consistently keep their response, it might indicate that they have important information or an important point of view.

B.1.3.2 Use

The Delphi technique is used for complex problems about which uncertainty exists and for which expert judgment is needed to deal with this uncertainty. It can be used in forecasting and policy making, and to obtain consensus or to reconcile differences between experts. It can be used to identify risks (with positive and negative outcomes), threats and opportunities and to gain consensus on the likelihood and consequences of future events. It is usually applied at a strategic or tactical level. Its original application was for long-time-frame forecasting, but it can be applied to any time frame.

B.1.3.3 Inputs

The method relies on the knowledge and continued cooperation of participants through a variable time scale that can be days, weeks, months or even years.

The number of participants can range from a few to hundreds. Written questionnaires can be in pencil-and-paper form or distributed and returned using electronic communication tools including email and the internet. The use of technology systems helps to ensure agility and precision in the compilation of information at each cycle.

B.1.3.4 Outputs

Consensus on the matter under consideration.

B.1.3.5 Strengths and limitations

Strengths include the following.

- As views are anonymous, unpopular opinions are more likely to be expressed and there is less hierarchy bias.
- All views have equal weight, which avoids the problem of dominating personalities.
- It achieves ownership of outcomes.
- People do not need to be brought together in one place at one time.
- People have time to make a considered response to the questions.
- The process tends to mean that experts devote their full attention to the task.

Limitations include the following.

- It is labour intensive and time consuming.
- Participants need to be able to express themselves clearly in writing.

B.1.3.6 Reference document

- [7] ROWE, G. WRIGHT, G. The Delphi technique: Past, present, and future prospects. *Technological forecasting and social change* 2011, 78, Special Delphi Issue

B.1.4 Nominal group technique**B.1.4.1 Overview**

The nominal group technique, like brainstorming, aims to collect ideas. Views are first sought individually with no interaction between group members, then are discussed by the group.

The process is as follows.

- The facilitator provides each group member with the questions to be considered.
- Individuals write down their ideas silently and independently.
- Each member of the group then presents their ideas with, at this stage, no discussion. If group dynamics mean that some voices have more weight than others, ideas can be passed on to the facilitator anonymously. Participants can then seek further clarification.
- Ideas are then discussed by the group to provide an agreed list.
- Members of the group vote privately on the ideas and a group decision is made based on the votes.

B.1.4.2 Use

The nominal group technique can be used as an alternative to brainstorming. It is also useful for prioritizing ideas within a group.

B.1.4.3 Inputs

The ideas and experiences of participants.

B.1.4.4 Outputs

Ideas, solutions or decisions as required.

B.1.4.5 Strengths and limitations

The strengths of the nominal group technique include the following.

- It provides a more balanced view than brainstorming when some members of a group are more vocal than others.
- It tends to produce more even participation if all or some group members are new to the team, the issue is controversial, or there is a power-imbalance or conflict amongst the team.
- It has been shown to generate a greater number of ideas than brainstorming.
- It diminishes pressure to conform to the group.
- It can achieve consensus in a relatively short time frame.

Limitations include the following.

- Cross fertilization of ideas can be constrained.
- The same ideas can be expressed in many slightly different ways, making them difficult to collate.

B.1.4.6 Reference document

- [8] MCDONALD, D. BAMMER, G. and DEANE, P. *Research Integration Using Dialogue Methods*

NOTE This reference also provides details of a range of other methods, some of which are also discussed in this document.

B.1.5 Structured or semi-structured interviews

B.1.5.1 Overview

In a structured interview, individual interviewees are asked a set of prepared questions. A semi-structured interview is similar, but allows more freedom for a conversation to explore issues which arise. In a semi-structured interview opportunity is explicitly provided to explore areas which the interviewee might wish to cover.

Questions should be open-ended where possible, should be simple, and in appropriate language for the interviewee, and each question should cover one issue only. Possible follow-up questions to seek clarification are also prepared.

The questions should be tested with people of similar background to those to be interviewed to check that the questions are not ambiguous, will be correctly understood and the answers will cover the issues intended. Care should be taken not to "lead" the interviewee.

B.1.5.2 Use

Structured and semi-structured interviews are a means of obtaining in-depth information and opinions from individuals in a group. Their answers can be confidential if necessary. They provide in-depth information where individuals are not biased by the views of other members of a group.

They are useful if it is difficult to get people together in the same place at the same time or if free-flowing discussion in a group is not appropriate for the situation or people involved. It is also possible to get more detailed information in an interview than is possible by survey or in a workshop situation. Interviews can be used at any level in an organization.

B.1.5.3 Inputs

The inputs are a clear understanding of the information required and a prepared set of questions which have been tested with a pilot group.

Those designing the interview and interviewers need some skills in order to obtain good valid responses that are not coloured by the interviewers' own biases.

B.1.5.4 Outputs

The output is the detailed information required.

B.1.5.5 Strengths and limitations

The strengths of structured interviews include the following.

- They allow people time for considered thought about an issue.
- One-to-one communication can allow more in-depth consideration of issues than a group approach.
- Structured interviews enable involvement of a larger number of stakeholders than a face-to-face group.

Limitations include the following.

- Interviews are time consuming to design, deliver and analyse.
- They require some expertise to design and deliver if answers are to be unbiased by the interviewer.
- Bias in the respondent is tolerated and is not moderated or removed through group discussion.
- Interviews do not trigger imagination (which is a feature of group methods).
- Semi-structured interviews produce a considerable body of information in the words of the interviewee. It can be difficult to group this unambiguously into a form amenable to analysis.

B.1.5.6 Reference documents

- [9] HARRELL, M.C. BRADLEY, M.A. 2009, *Data collection methods – A training Manual – Semi structured interviews and focus groups*
- [10] GILL, J. JOHNSON, P. 2010, *Research methods for managers*

B.1.6 Surveys

B.1.6.1 Overview

Surveys generally engage more people than interviews and usually ask more restricted questions. Typically, a survey will involve a computer- or paper-based questionnaire. Questions often offer yes/no answers, choices from a rating scale or choices from a range of options. This allows statistical analysis of the results, which is a feature of such methods. Some questions with free answers can be included, but their number should be limited because of analysis difficulties.

B.1.6.2 Use

Surveys can be used in any situation where wide stakeholder consultation is useful, particularly when relatively little information is needed from a large number of people.

B.1.6.3 Inputs

Pre-tested, unambiguous questions sent to a broadly representative sample of people willing to participate. The number of responses needs to be sufficient to provide statistical validity. (Return rates are often low, meaning many questionnaires need to be sent out.) Some expertise is needed in developing a questionnaire that will achieve useful results and in the statistical analysis of results.

B.1.6.4 Outputs

The output is an analysis of the views from a range of individuals, often in graphical form.

B.1.6.5 Strengths and limitations

The strengths of surveys include the following.

- Larger numbers can be involved than for interviews, providing better information across a group.
- Surveys are relatively low cost to run, especially if online software is used that is capable of providing some statistical analysis.
- They can provide statistically valid information.
- Results are easy to tabulate and easy to understand: graphical output is usually possible.
- Reports of surveys can be made available to others relatively easily.

Limitations include the following.

- The nature of questions is restricted by the need to be simple and unambiguous.
- It is usually necessary to obtain some demographic information in order to interpret results.
- The number of questions that can be included is limited if a sufficient number of responses is to be expected.
- The person posing the question cannot explain, so respondents may interpret questions differently than was intended.
- It is difficult to design questions that do not lead respondents to particular answers.
- Questionnaires tend to have underlying assumptions that might not be valid.
- It can be difficult to obtain a good and unbiased response rate.

B.1.6.6 Reference documents

- [11] SAUNDERS, M. LEWIS, P. THORNHILL, A. 2016, *Research Methods for Business Students*
- [12] UNIVERSITY OF KANSAS COMMUNITY TOOL BOX Section 13, *Conducting surveys*

B.2 Techniques for identifying risk

B.2.1 General

Risk identification techniques can include:

- evidence based methods, such as literature reviews, and analysis of historical data;
- empirical methods, including testing and modelling to identify what might happen under particular circumstances;
- perception surveys, which canvas the views of a wide range of experienced people;
- techniques in which the subject being considered is divided into smaller elements each of which is considered in turn using methods which raise what if questions;

EXAMPLES HAZOP (B.2.4), FMEA (B.2.3) and SWIFT(B.2.6).

- techniques for encouraging imaginative thinking about possibilities of the future, such as scenario analysis (B.2.5);
- checklists or taxonomies based on past data or theoretical models (B.2.2).

The techniques described in Clause B.2 are examples of some structured approaches to identifying risk. A structured technique is likely to be more comprehensive than an unstructured

or semi-structured workshop and be more easily used to demonstrate due diligence in identifying risk.

The use of multiple techniques including both top down and bottom up methods encourages comprehensive risk identification. Approaches which challenge outcomes of risk identification such as red teaming can also be used to help check no relevant risks have been overlooked.

NOTE Red teaming is the practice of viewing a problem from an adversary's or competitor's perspective [13].

The techniques described can involve multiple stakeholders and experts. Methods that can be used to elicit views, either individually or in a group, are described in Clause B.1.

B.2.2 Checklists, classifications and taxonomies

B.2.2.1 Overview

Checklists are used during risk assessment in various ways such as to assist in understanding the context, in identifying risk and in grouping risks for various purposes during analysis. They are also used when managing risk, for example to classify controls and treatments, to define accountabilities and responsibilities, or to report and communicate risk.

A checklist can be based on experience of past failures and successes but more formally risk typologies and taxonomies can be developed to categorize or classify risks based on common attributes. In their pure forms, typologies are "top-down" conceptually derived classification schemes whereas taxonomies are "bottom-up" empirically or theoretically derived classification schemes. Hybrid forms typically blend these two pure forms.

Risk taxonomies are typically intended to be mutually exclusive and collectively exhaustive (i.e. to avoid overlaps and gaps). Risk classifications can focus on isolating a particular category of risk for closer examination.

Both typologies and taxonomies can be hierarchical with several levels of classification developed. Any taxonomy should be hierarchical and be able to be subdivided to increasingly fine levels of resolution. This will help maintain a manageable number of categories while also achieving sufficient granularity.

B.2.2.2 Use

Checklists, classifications and taxonomies can be designed to apply at strategic or operational level. They can be applied using questionnaires, interviews, structured workshops, or combinations of all three, in face-to-face or computer-based methods.

Examples of commonly used checklists, classifications or taxonomies used at a strategic level include the following.

- SWOT (strengths, weaknesses, opportunities and threats) identifies factors in the internal and external context to assist with setting objectives and the strategies to achieve them taking account of risk.
- PESTLE, STEEP, STEEPLED, etc. are acronyms representing types of factor to consider when establishing the context or identifying risks [14]. The letters represent Political, Economic, Social, Technological, Environmental, Legal, Ethical and Demographic. Categories relevant to the particular situation can be selected and checklists developed for examples under each category.
- Consideration of strategic objectives, critical success factors for reaching objectives, threats to success factors and risk drivers. From this, risk treatments and early warning indicators for the risk drivers can be developed.

At an operational level, hazard checklists are used to identify hazards within HAZID and Preliminary Hazard Analysis (PHA) [15]. These are preliminary safety risk assessments usually carried out at the early design stage of a project.

General categorizations of risk include:

- by source of risk: market prices, counterparty default, fraud, safety hazards, etc.;
- by consequence, aspects or dimensions of objectives or performance.

Pre-identified categories of risk can be useful in directing thinking about risk across a broad range of issues. However it is difficult to ensure such categories are comprehensive, and by subdividing risk in a predefined way, thinking is directed along particular lines and important aspects of risk might be overlooked.

Checklists, typologies and taxonomies are used within other techniques described in this document; for example, the key words in HAZOP B.2.4 and the categories in an Ishikawa analysis (B.3.3). A taxonomy that can be used to consider human factors when identifying risk is given in IEC 62740:2015 [16].

In general, the more specific the checklist, the more restricted its use to the particular context in which it is developed. Words that provide general prompts are usually more productive in encouraging a level of creativity when identifying risk.

B.2.2.3 Inputs

Inputs are data or models from which to develop valid checklists, taxonomies or classifications.

B.2.2.4 Outputs:

Outputs are:

- checklists, prompts or categories and classification schemes;
- an understanding of risk from the use of these, including (in some cases) lists of risks and groupings of risks.

B.2.2.5 Strengths and limitations

Strengths of checklists, taxonomies, typographies include the following.

- They promote a common understanding of risk among stakeholders.
- When well designed, they bring wide ranging expertise into an easy to use system for non-experts.
- Once developed they require little specialist expertise.

Limitations include the following.

- Their use is limited in novel situations where there is no relevant past history or in situations that differ from that for which they were developed.
- They address what is already known or imagined.
- They are often generic and might not apply to the particular circumstances being considered.
- Complexity can hinder identification of relationships (e.g., interconnections and alternative groupings).
- Lack of information can lead to overlaps and/or gaps (e.g. schemes are not mutually exclusive and collectively exhaustive).
- They can encourage "tick the box" type of behaviour rather than exploration of ideas.

B.2.2.6 Reference documents

- [17] BROUGHTON, Vanda, *Essential classification*
- [18] BAILEY, Kenneth, *Typologies and taxonomies: An introduction to classification techniques*
- [19] VDI 2225 Blatt 1, Konstruktionsmethodik- Technisch-wirtschaftliches Konstruieren - Vereinfachte Kostenermittlung, 1997 Beuth Verlag

B.2.3 Failure modes and effects analysis (FMEA) and failure modes, effects and criticality analysis (FMECA)

B.2.3.1 Overview

In FMEA, a team subdivides hardware, a system, a process or a procedure into elements. For each element the ways in which it might fail, and the failure causes and effects are considered. FMEA can be followed by a criticality analysis which defines the significance of each failure mode (FMECA).

For each element the following is recorded:

- its function;
- the failure that might occur (failure mode);
- the mechanisms that could produce these modes of failure;
- the nature of the consequences if failure did occur;
- whether the failure is harmless or damaging;
- how and when the failure can be detected;
- the inherent provisions that exist to compensate for the failure.

For FMECA, the study team classifies each of the identified failure modes according to its criticality. Several different methods of criticality can be used. The most frequently used are a qualitative, semi-quantitative or quantitative consequence/likelihood matrix (B.10.3) or a risk priority number (RPN). A quantitative measure of criticality can also be derived from actual failure rates and a quantitative measure of consequences where these are known.

NOTE The RPN is an index method (B.8.6) that takes the product of ratings for consequence of failure, likelihood of failure and ability to detect the problem (detection). A failure is given a higher priority if it is difficult to detect.

B.2.3.2 Use

FMEA/FMECA can be applied during the design, manufacture or operation of a physical system to improve design, select between design alternatives or plan a maintenance programme. It can also be applied to processes and procedures, such as in medical procedures and manufacturing processes. It can be performed at any level of breakdown of a system from block diagrams to detailed components of a system or steps of a process.

FMEA can be used to provide information for analysis techniques such as fault tree analysis. It can provide a starting point for a root cause analysis.

B.2.3.3 Inputs

Inputs include information about the system to be analysed and its elements in sufficient detail for meaningful analysis of the ways in which each element can fail and the consequences if it does. The information needed can include drawings and flow charts, details of the environment in which the system operates, and historical information on failures where available.

FMEA is normally carried out by a cross functional team with expert knowledge of the system being analysed, led by a trained facilitator. It is important for the team to cover all relevant areas of expertise.

B.2.3.4 Outputs

The outputs of FMEA are:

- a worksheet with failure modes, effects, causes and existing controls;
- a measure of the criticality of each failure mode (if FMECA) and the methodology used to define it;
- any recommended actions, e.g. for further analyses, design changes or features to be incorporated in test plans.

FMECA usually provides a qualitative ranking of the importance of failure modes, but can give a quantitative output if suitable failure rate data and quantitative consequences are used.

B.2.3.5 Strengths and limitations

The strengths of FMEA/FMECA include the following.

- It can be applied widely to both human and technical modes of systems, hardware, software and procedures.
- It identifies failure modes, their causes and their effects on the system, and presents them in an easily readable format.
- It avoids the need for costly equipment modifications in service by identifying problems early in the design process.
- It provides input to maintenance and monitoring programmes by highlighting key features to be monitored.

Limitations include the following.

- FMEA can only be used to identify single failure modes, not combinations of failure modes.
- Unless adequately controlled and focused, the studies can be time consuming and costly.
- FMEA can be difficult and tedious for complex multi-layered systems.

B.2.3.6 Reference document

[20] IEC 60812, *Failure modes and effects analysis (FMEA and FMECA)*

B.2.4 Hazard and operability (HAZOP) studies

B.2.4.1 Overview

A HAZOP study is a structured and systematic examination of a planned or existing process, procedure or system that involves identifying potential deviations from the design intent, and examining their possible causes and consequences.

Within a facilitated workshop, the study team:

- subdivides the system, process or procedure into smaller elements;
- agrees the design intent for each element including defining relevant parameters (such as flow or temperature in the case of a physical system);
- applies guidewords successively to each parameter for each element to postulate possible deviations from the design intent that could have undesirable outcomes;

NOTE Not all guideword parameter combinations will be meaningful.

- agrees the cause and consequences in each case suggesting how they might be treated;
- documents the discussion and agrees possible actions to treat the risks identified.

Table B.1 provides examples of commonly used guidewords for technical systems. Similar guidewords such as "too early", "too late", "too much", "too little", "too long", "too short", "wrong direction", "wrong object", "wrong action" can be used to identify human error modes.

Guidewords are applied to parameters such as:

- physical properties of a material or process;
- physical conditions such as temperature or speed;
- timing;
- a specified intention of a component of a system or design (e.g. information transfer);
- operational aspects.

Table B.1 – Examples of basic guidewords and their generic meanings

Guideword	Definition
No or not	No part of the intended result is achieved or the intended condition is absent
More (higher)	Quantitative increase
Less (lower)	Quantitative decrease
As well as	Qualitative modification/increase (e.g. additional material)
Part of	Qualitative modification/decrease (e.g. only one of two components in a mixture)
Reverse/opposite	Logical opposite of the design intent (e.g. backflow)
Other than	Complete substitution, something completely different happens (e.g. wrong material)
Early	Relative to clock time
Late	Relative to clock time

B.2.4.2 Use

HAZOP studies were initially developed to analyse chemical process systems, but have been extended to other types of system including mechanical, electronic and electrical power systems, software systems, organizational changes, human behaviour and legal contract design and review.

The HAZOP process can deal with all forms of deviation from design intent due to deficiencies in the design, component(s), planned procedures and human actions. It is most often used to improve a design or identify risks associated with a design change. It is usually undertaken at the detail design stage, when a full diagram of the intended process and supporting design information are available, but while design changes are still practicable. It can however, be carried out in a phased approach with different guidewords for each stage as a design develops in detail. A HAZOP study can also be carried out during operation but required changes can be costly at that stage.

B.2.4.3 Inputs

Inputs include current information about the system to be reviewed and the intention and performance specifications of the design. For hardware this can include drawings, specification sheets, flow diagrams, process control and logic diagrams, and operating and maintenance procedures. For non-hardware related HAZOP, the inputs can be any document that describes functions and elements of the system or procedure under study, for example, organizational diagrams and role descriptions, or a draft contract or draft procedure.

A HAZOP study is usually undertaken by a multidisciplinary team that should include designers and operators of the system as well as persons not directly involved in the design or the system, process or procedure under review. The leader/facilitator of the study should be trained and experienced in handling HAZOP studies.

B.2.4.4 Outputs

Outputs include minutes of the HAZOP meeting(s) with deviations for each review point recorded. Records should include the guideword used, and possible causes of deviations. They can also include actions to address the identified problems and the person responsible for the action.

B.2.4.5 Strengths and limitations

Strengths of HAZOP include the following.

- It provides the means to systematically examine a system, process or procedure to identify how it might fail to achieve its purpose.
- It provides a detailed and thorough examination by a multidisciplinary team.
- It identifies potential problems at the design stage of a process.
- It generates solutions and risk treatment actions.
- It is applicable to a wide range of systems, processes and procedures.
- It allows explicit consideration of the causes and consequences of human error.
- It creates a written record of the process, which can be used to demonstrate due diligence.

Limitations include the following.

- A detailed analysis can be time consuming and therefore expensive.
- The technique tends to be repetitive, finding the same issues multiple times; hence it can be difficult to maintain concentration.
- A detailed analysis requires a high level of documentation or system/process and procedure specification.
- It can focus on finding detailed solutions rather than on challenging fundamental assumptions (however, this can be mitigated by a phased approach).
- The discussion can be focused on detail issues of design, and not on wider or external issues.
- It is constrained by the (draft) design and design intent, and the scope and objectives given to the team.
- The process relies heavily on the expertise of the designers who might find it difficult to be sufficiently objective to seek problems in their designs.

B.2.4.6 Reference document

[21] IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

B.2.5 Scenario analysis

B.2.5.1 Overview

Scenario analysis is a name given to a range of techniques that involve developing models of how the future might turn out. In general terms, it consists of defining a plausible scenario and working through what might happen given various possible future developments.

For relatively short time scales it can involve extrapolating from what has happened in the past. For longer time scales, scenario analysis can involve building an imaginary but credible scenario then exploring the nature of risks within this scenario. It is most often applied by a group of stakeholders with different interests and expertise. Scenario analysis involves defining in some detail the scenario or scenarios to be considered and exploring the implications of the scenario and associated risk. Changes commonly considered include:

- changes in technology;
- possible future decisions that might have a variety of outcomes;
- stakeholder needs and how they might change;
- changes in the macro environment (regulatory, demographics, etc.);
- changes in the physical environment.

B.2.5.2 Use

Scenario analysis is most often used to identify risk and explore consequences. It can be used at both strategic and operational level, for the organization as a whole or part of it.

Long-term scenario analysis attempts to aid planning for major shifts in the future such as those that have occurred over the past 50 years in technology, consumer preferences, social attitudes, etc. Scenario analysis cannot predict the probabilities of such changes but can consider consequences and help organizations develop strengths and the resilience needed to adapt to foreseeable change. It can be used to anticipate how both threats and opportunities might develop and can be used for all types of risk.

Short-time-frame scenario analysis is used to explore the consequences of an initiating event. Likely scenarios can be extrapolated from what has happened in the past or from models. Examples of such applications include planning for emergency situations or business interruptions. If data are not available, experts' opinions are used, but in this case it is very important to give utmost attention to their explanations for their views.

B.2.5.3 Inputs

To undertake a scenario analysis, data on current trends and changes and ideas for future change are required. For complex or very long-term scenarios, expertise in the technique is required.

B.2.5.4 Outputs

The output can be a "story" for each scenario that tells how one might move from the present towards the subject scenario. The effects considered can be both beneficial and detrimental. The stories may include plausible details that add value to the scenarios.

Other outputs can include an understanding of possible effects of policy or plans for various plausible futures, a list of risks that might emerge if the futures were to develop and, in some applications, a list of leading indicators for those risks.

B.2.5.5 Strengths and limitations

Strengths of scenario analysis include the following.

- It takes account of a range of possible futures. This can be preferable to the traditional approach of relying on forecasts that assume that future events will probably continue to follow past trends. This is important for situations where there is little current knowledge on which to base predictions or where risks are being considered in the longer term.
- It supports diversity of thinking.
- It encourages monitoring of lead indicators of change.
- Decisions made for the risks identified can help build resilience for whatever does occur.

Limitations include the following.

- The scenarios used might not have an adequate foundation, for example data might be speculative. This could produce unrealistic results that might not be recognized as such.

- There is little evidence that scenarios explored for the long-term future are those that actually occur.

B.2.5.6 Reference documents

- [22] RINGLAND, Gill. *Scenarios in business*
- [23] Van der HEIJDEN, Kees. *Scenarios: The art of strategic conversation*
- [24] CHERMACK, Thomas J. *Scenario planning in organizations*
- [25] MUKUL PAREEK, *Using Scenario analysis for managing technology risk*

B.2.6 Structured what if technique (SWIFT)

B.2.6.1 Overview

SWIFT is a high-level risk identification technique that can be used independently, or as part of a staged approach to make bottom-up methods such as HAZOP or FMEA more efficient. SWIFT uses structured brainstorming (B.1.2) in a facilitated workshop where a predetermined set of guidewords (timing, amount, etc.) are combined with prompts elicited from participants that often begin with phrases such as "what if?" or "how could?". It is similar to HAZOP but applied at a system or subsystem rather than on the designer's intent.

Before the study commences the facilitator prepares a prompt list to enable a comprehensive review of risks or sources of risk. At the start of the workshop the context, scope and purpose of the SWIFT is discussed and criteria for success articulated. Using the guidewords and "what if?" prompts, the facilitator asks the participants to raise and discuss issues such as:

- known risks;
- risk sources and drivers;
- previous experience, successes and incidents;
- known and existing controls;
- regulatory requirements and constraints.

The facilitator uses the prompt list to monitor the discussion and to suggest additional issues and scenarios for the team to discuss. The team considers whether controls are adequate and if not considers potential treatments. During this discussion, further "what if?" questions are posed.

In some cases specific risks are identified and a description of the risk, its causes, consequences and controls can be recorded. In addition, more general sources or drivers of risk, control problems or systemic issues may be identified.

Where a list of risks is generated a qualitative or semi-quantitative risk assessment method is often used to rank the actions created in terms of level of risk. This normally takes into account the existing controls and their effectiveness.

B.2.6.2 Use

The technique can be applied to systems, plant items, procedures and organizations generally. In particular, it is used to examine the consequences of changes and the risk thereby altered or created. Both positive and negative outcomes can be considered. It can also be used to identify the systems or processes for which it would be worth investing the resources for a more detailed HAZOP or FMEA.

B.2.6.3 Inputs

A clear understanding of the system, procedure, plant item and/or change and the external and internal contexts is needed. This is established through interviews, gathering a multifunctional team and through the study of documents, plans and drawings by the facilitator. Normally the

system for study is split into elements to facilitate the analysis process. Although the facilitator needs to be trained in the application of SWIFT, this can usually be quickly accomplished.

B.2.6.4 Outputs

Outputs include a register of risks with risk-ranked actions or tasks that can be used as the basis for a treatment plan.

B.2.6.5 Strengths and limitations

Strengths of SWIFT include the following.

- It is widely applicable to all forms of physical plant or system, situation or circumstance, organization or activity.
- It needs minimal preparation by the team.
- It is relatively rapid and the major risks and risk sources quickly become apparent within the workshop session.
- The study is "systems orientated" and allows participants to look at the system response to deviations rather than just examining the consequences of component failure.
- It can be used to identify opportunities for improvement of processes and systems and generally can be used to identify actions that lead to and enhance their probabilities of success.
- Involvement in the workshop by those who are accountable for existing controls and for further risk treatment actions reinforces their responsibility.
- It creates a risk register and risk treatment plan with little more effort.

Limitations include the following.

- If the workshop team does not have a wide enough experience base or if the prompt system is not comprehensive, some risks or hazards might not be identified.
- The high-level application of the technique might not reveal complex, detailed or correlated causes.
- Recommendations are often generic, e.g. the method does not provide support for robust and detailed controls without further analysis being carried out.

B.2.6.6 Reference document

- [26] CARD, Alan J. WARD, James R. and CLARKSON, P. John. Beyond FMEA: The structured what-if technique (SWIFT)

B.3 Techniques for determining sources, causes and drivers of risk

B.3.1 General

An understanding of the causes of potential events and the drivers of risk can be used to design strategies to prevent adverse consequences or enhance positive ones. Often there is a hierarchy of causes with several layers before the root cause is reached. Generally causes are analysed until actions can be determined and justified.

Causal analysis techniques can explore perceptions of cause under a set of predetermined headings such as in the Ishikawa method (see B.3.3), or can take a more logic based approach as in fault tree analysis and success tree analysis (see B.5.7).

Bow tie analysis (see B.4.2) can be used to represent causes and consequences graphically, and show how they are controlled.

Several of the techniques described in IEC 62740 [16] can be used proactively to analyse possible causes of events that might happen in the future, as well as those that have already occurred. These techniques are not repeated here.

B.3.2 Cindynic approach

B.3.2.1 Overview

Cindynics literally means the science of danger. The cindynic approach identifies intangible risk sources and drivers that might give rise to many different consequences. In particular, it identifies and analyses:

- inconsistencies, ambiguities, omissions, ignorance (termed deficits), and
- divergences between stakeholders (termed dissonances).

The cindynic approach starts by collecting information on the system or organization which is the subject of the study and the cindynic situation defined by a geographical, temporal and chronological space and a set of stakeholder networks or groups.

It then uses semi-structured interviews (see B.1.5) to collect information at various times ($t_1, t_2, \dots, t_i$) about the state of knowledge, and the state of mind, of each stakeholder, as they relate to the five criteria of the cindynic approach as follows:

- goal (primary purpose of the organization);
- values (considered in high esteem by the stakeholder);
- rules (rights, standards, procedures, etc. governing its achievements);
- data (on which decision making is based);
- models (technical, organizational, human, etc., that use data in decision making).

NOTE The elements characterizing internal and external contexts can be put together according to the five criteria of the cindynic approach.

The approach takes into account perceptions as well as facts.

Once this information is obtained, the coherence between objectives to be reached and the five criteria of cindynics are analysed and tables are set up listing deficits and dissonances.

B.3.2.2 Use

The aim of the cindynic approach is to understand why, despite all the control measures taken to prevent disasters, they still happen. The approach has since been extended to improve the economic efficiency of organizations. The technique seeks systemic sources and drivers of risk within an organization which can lead to wide ranging consequences. It is applied at a strategic level and can be used to identify factors acting in a favourable or unfavourable way during the evolution of the system towards new objectives.

It can also be used to validate the consistency of any project and is especially useful in the study of complex systems.

B.3.2.3 Inputs

Information as described above. The analysis usually involves a multidisciplinary team including those with real-life operational experience and those who will carry out treatment actions to address the sources of risk identified.

B.3.2.4 Outputs

The outputs are tables which indicate dissonances and deficits between stakeholders, as illustrated in the examples below. Table B.2 shows a matrix indicating the deficits of each stakeholder against the five criteria for analysis (goals, values, rules, models, and data). By comparing the information gathered as input between situations taken at times $t_1, t_2, \dots, t_i$, it is possible to identify deficits between different situations.

Table B.2 – Table of deficits for each stakeholder

Stakeholder	Criterion for analysis				
	Goals	Values	Rules	Data	Models
S1		Focus on a restricted number of values	No reference to procedures	No reference to measurements	No reference to models
S2	Inconsistency between goals and rules	Lack of ranking between values	Lack of ranking between rules	Ignorance of experience and feedback from other countries	Ignorance of specific models
S3	Inconsistency between goals and standards	Focus on a specific value (e.g. employment)	Lack of ranking between rules	No attention paid to specific data e.g. occupational injuries)	Lack of prioritization in selecting models

Table B.3 is a matrix where relevant stakeholders are represented on both axes and the difference in views between stakeholders (so called dissonances) are shown in the matrix cells. These tables enable a programme for reduction of deficits and dissonances to be established.

Table B.3 – Table of dissonances between stakeholders

Stakeholder	Stakeholder			
	S1	S2	S3	S4
S1		S1 and S2 do not share the same goals	S1 and S3 do not share the same values	S1 and S4 do not share the same measurement systems
S2			S2 and S3 do not agree on interpretation of procedures	S2 and S4 do not agree on data
S3				S3 and S4 disagree on interpretation of rules
S4				

B.3.2.5 Strengths and limitations

Strengths of the cindynic approach include the following.

- It is a systemic, multidimensional and multidisciplinary approach.
- It provides knowledge of the potential riskiness of a system and its consistency.
- It considers human and organizational aspects of risk at any level of responsibility.
- It integrates space and time notions.
- It yields solutions to reduce risks.

Limitations include the following.

- It does not attempt to prioritize sources of risk or risks.
- It has only recently begun to be disseminated in industry. It therefore does not benefit from the same maturity acquired through past developments as traditional approaches.
- Depending on the number of stakeholders involved, it can require significant time and resources.

B.3.2.6 Reference documents

[27] KERVERN, G-Y. Elements fondamentaux des cindyniques

[28] KERVERN, G-Y. Latest advances in cindynics

[29] KERVERN, G-Y. & BOULENGER, P. Cindyniques – Concepts et mode d'emploi

B.3.3 Ishikawa analysis (fishbone) method

B.3.3.1 Overview

Ishikawa analysis uses a team approach to identify possible causes of any desirable or undesirable event, effect, issue or situation. The possible contributory factors are organized into broad categories to cover human, technical and organizational causes. The information is depicted in a fishbone (also called Ishikawa) diagram (see Figure B.1). The main steps in performing the analysis are the following.

- Establish the effect to be analysed and place it in a box as the head of the fishbone diagram. The effect can be either positive (an objective) or negative (a problem);
- Agree on the main categories of causes. Examples of commonly used categories include:
 - 6Ms, for example, methods, machinery, management, materials, manpower, money;
 - materials, methods and processes, environment, equipment, people, measurements.

NOTE Any set of agreed categories can be used that fit the circumstances being analysed. Figure B.1 illustrates another possibility.

- Ask "why?" and "how might that occur?" iteratively to explore the causes and influencing factors in each category, adding each to the bones of the fishbone diagram.
- Review all branches to verify consistency and completeness and ensure that the causes apply to the main effect.
- Identify the most important factors based on the opinion of the team and available evidence.

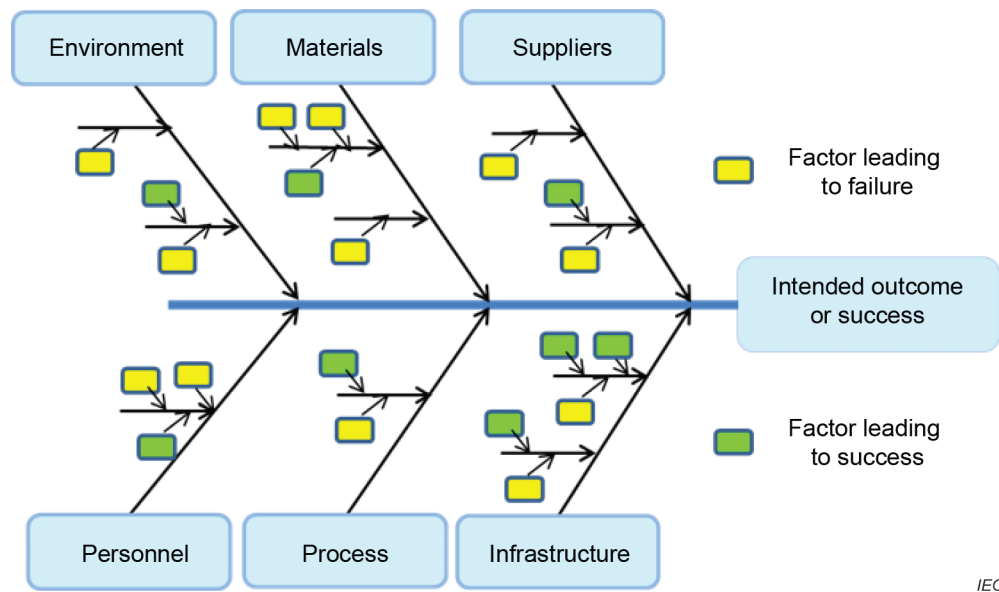


Figure B.1 – Example Ishikawa (fishbone) diagram

The diagram is often developed in a workshop scenario.

B.3.3.2 Use

Ishikawa analysis can be used when performing a root cause analysis of events which have occurred, or to identify factors that might contribute to outcomes which have not yet occurred. The method can be used to examine situations at any level in an organization over any time scale.

The diagrams are generally used qualitatively. It is possible to assign probabilities to generic causes, and subsequently to the sub-causes, on the basis of the degree of belief about their relevance. However, contributory factors often interact and contribute to the effect in complex ways and there can be unidentified causes, which make quantification invalid.

B.3.3.3 Input

The input is the expertise and experience of participants and an understanding of the situation under examination.

B.3.3.4 Output

The output is perceived causes of the effect being analysed, normally displayed as a fishbone or Ishikawa diagram. The fishbone diagram is structured by representing the main categories as major bones off the fish backbone with branches and sub-branches that describe more specific sub-causes in those categories.

B.3.3.5 Strengths and limitations

Strengths of the Ishikawa technique include the following.

- It encourages participation and utilizes group knowledge.
- It provides a focused approach for brainstorming or similar identification techniques.
- It can be applied to a wide range of situations.
- It provides a structured analysis of cause with an easy to read graphical output.
- It allows people to report problems in a neutral environment.
- It can be used to identify contributory factors to wanted as well as unwanted effects.

NOTE A positive focus can encourage greater ownership and participation.

Limitations include the following.

- The separation of causal factors into major categories at the start of the analysis means that interactions between the categories might not be considered adequately.
- Potential causes not covered by the categories selected are not identified.

B.3.3.6 Reference documents

[30] ISHIKAWA, K. Guide to Quality Control

See also IEC 62740 [16] for other causal analysis techniques.

B.4 Techniques for analysing controls

B.4.1 General

The techniques in Clause B.4 can be used to check whether controls are appropriate and adequate.

Bow tie analysis (B.4.2) and LOPA (B.4.4) identify the barriers between a source of risk and its possible consequences and can be used to check that the barriers are sufficient.

HACCP (B.4.3) seeks points in a process where conditions can be monitored and controls introduced when there is an indication that the conditions are changing.

Event tree analysis (B.5.6) can also be used as a quantitative means of controls analysis by calculating the influence of different controls on the probability of consequences.

Any causal analysis technique can be used as a basis for checking that each cause is controlled.

B.4.2 Bow tie analysis

B.4.2.1 Overview

A bow tie is a graphical depiction of pathways from the causes of an event to its consequences. It shows the controls that modify the likelihood of the event and those that modify the consequences if the event occurs. It can be considered as a simplified representation of a fault tree or success tree (analysing the cause of an event) and an event tree (analysing the consequences). Bow tie diagrams can be constructed starting from fault and event trees, but are more often drawn directly by a team in a workshop scenario.

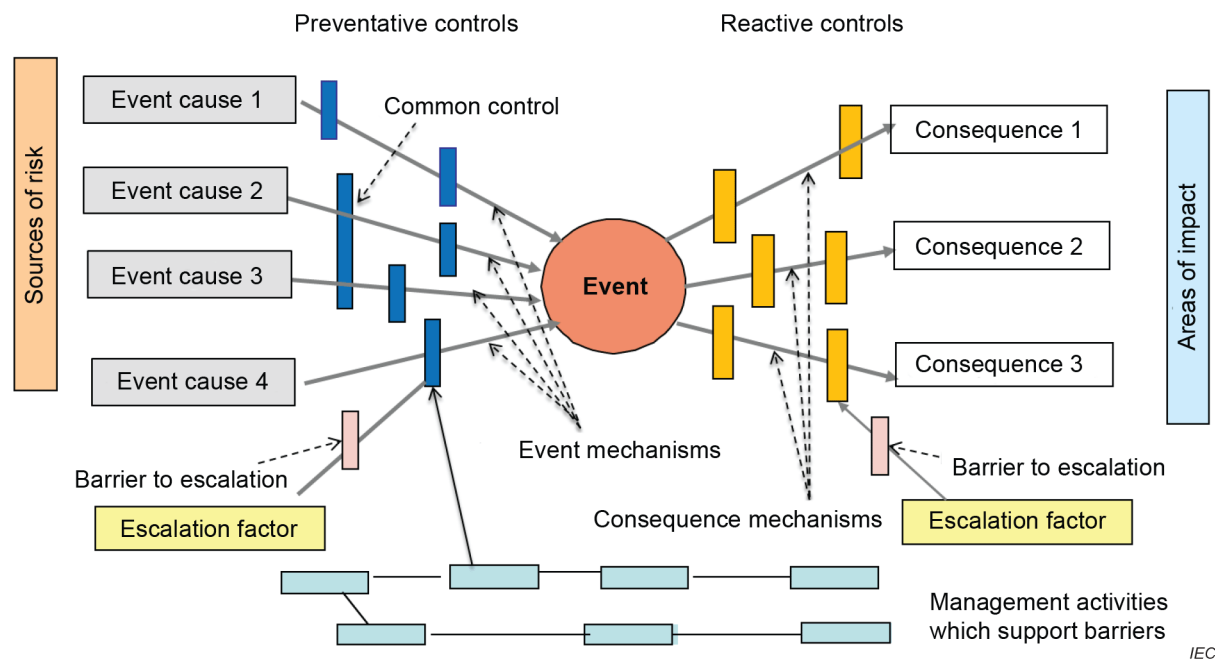


Figure B.2 – Example of Bowtie

The bow tie is drawn as follows.

- The event of interest is represented by the central knot of the bow tie, see Figure B.2.
- Sources of risk (or hazards/threats in a safety context) are listed on the left hand side of the knot and joined to the knot by lines representing the different mechanisms by which sources of risk can lead to the event.
- Barriers or controls for each mechanism are shown as vertical bars across the lines.
- On the right-hand side of the knot lines are drawn to radiate out from the event to each potential consequence.
- After the event vertical bars represent reactive controls or barriers that modify consequences.
- Factors that might cause the controls to fail (escalation factors) are added, together with controls for the escalation factors.
- Management functions which support controls (such as training and inspection) can be shown under the bow tie and linked to the respective control.

Some level of quantification of a bow tie diagram can be possible where pathways are independent, the probability of a particular consequence or outcome is known and the probability that a control will fail can be estimated. However, in many situations, pathways and barriers are not independent, and controls may be procedural and their effectiveness uncertain. Quantification is often more appropriately carried out using fault tree analysis (B.5.7) and event tree analysis (B.5.6) or LOPA (B.4.4).

B.4.2.2 Use

Bow tie analysis is used to display and communicate information about risks in situations where an event has a range of possible causes and consequences. It can be used to explore in detail the causes and consequences of events that are recorded in a simple form in a risk register (B.10.2). It is particularly used for analysing events with more serious consequences. A bow tie is used when assessing controls to check that each pathway from cause to event and event to consequence has effective controls, and that factors that could cause controls to fail (including management systems failures) are recognized. It can be used as the basis of a means to record information about a risk that does not fit the simple linear representation of a risk register. It

can be used proactively to consider potential events and also retrospectively to model events that have already occurred.

The bow tie is used when the situation does not warrant the complexity of a full fault tree analysis and event tree analysis but is more complex than can be represented by a single cause-event-consequence pathway.

For some situations cascading bow ties can be developed where the consequences of one event become the cause of the next.

B.4.2.3 Input

Input includes information about the causes and consequences of the pre-defined event, and the controls that might modify it. This information may be taken from the output of techniques to identify risks and controls or from the experience of individuals.

B.4.2.4 Output

The output is a simple diagram showing main risk pathways, the controls in place, and the factors that might lead to control failure. It also shows potential consequences and the measures that can be taken after the event has occurred to modify them.

B.4.2.5 Strengths and limitations

Strengths of bow tie analysis include the following.

- It is simple to understand and gives a clear pictorial representation of an event and its causes and consequences.
- It focuses attention on controls which are supposed to be in place and their effectiveness.
- It can be used for desirable consequences as well as undesirable ones.
- It does not need a high level of expertise to use.

Limitations include the following.

- A bow tie cannot depict a situation where pathways from causes to the event are not independent (i.e. where there would be AND gates in a fault tree).
- It can over-simplify complex situations particularly where quantification is attempted.

B.4.2.6 Reference documents

- [31] LEWIS, S. SMITH, K., *Lessons learned from real world application of the bow-tie method.* [31]
- [32] HALE, A. R., GOOSSENS L.H.J., ALE, B.J.M., BELLAMY L.A. POST J. *Managing safety barriers and controls at the workplace*
- [33] MCCONNELL, P. and DAVIES, M. *Scenario Analysis under Basel II*

B.4.3 Hazard analysis and critical control points (HACCP)

B.4.3.1 Overview

Hazard analysis and critical control points (HACCP) was developed to ensure food safety for the NASA space program but can be used for non-food processes or activities. The technique provides a structure for identifying sources of risk (hazards or threats) and putting controls in place at all relevant parts of a process to protect against them. HACCP is used at operational levels although its results can support the overall strategy of an organization. HACCP aims to ensure that risks are minimized by monitoring and by controls throughout a process rather than through inspection at the end of the process.

HACCP consists of the following seven principles:

- 1) identify hazards, the factors which influence the risk and possible preventive measures;
- 2) determine the points in the process where monitoring is possible and the process can be controlled to minimize threats (the critical control points or CCPs);
- 3) establish critical limits for the parameters which are to be monitored, i.e. each CCP should operate within specific parameters to ensure the risk is controlled;
- 4) establish the procedures to monitor critical limits for each CCP at defined intervals;
- 5) establish corrective actions to be used when the process falls outside established limits;
- 6) establish verification procedures;
- 7) implement record keeping and documentation procedures for each step.

B.4.3.2 Use

HACCP is a requirement in most countries for organizations operating anywhere within the food chain, from harvesting to consumption, to control risks from physical, chemical or biological contaminants.

It has been extended for use in manufacture of pharmaceuticals, medical devices and in other areas where the biological, chemical and physical risks are inherent to the organization.

The principle of the technique is to identify sources of risk related to the quality of the output of a process, and to define points in that process where critical parameters can be monitored and sources of risk controlled. This can be generalized to many other processes, including for example financial processes.

B.4.3.3 Inputs

Inputs include:

- a basic flow diagram or process diagram;
- information on sources of risk that might affect the quality, safety or reliability of the product or process output;
- information on the points in the process where indicators can be monitored and controls can be introduced.

B.4.3.4 Outputs

Outputs include records, including a hazard analysis worksheet and a HACCP plan.

The hazard analysis worksheet lists for each step of the process:

- hazards which could be introduced, controlled or exacerbated at that step;
- whether the hazards present a significant risk (based on consideration of consequence and probability using a combination of experience, data and technical literature);
- a justification for the significance rating;
- possible preventative measures for each hazard;
- whether monitoring or control measures can be applied at this step (i.e. is it a CCP?).

The HACCP plan delineates the procedures to be followed to assure the control of a specific design, product, process or procedure. The plan includes a list of all CCPs and for each CCP lists:

- the critical limits for preventative measures;
- monitoring and continuing control activities (including what, how, and when monitoring will be carried out and by whom);
- corrective actions required if deviations from critical limits are detected;

- verification and record-keeping activities.

B.4.3.5 Strengths and limitations

Strengths of HACCP include the following.

- HACCP is a structured process that provides documented evidence for quality control as well as identifying and reducing risks.
- It focuses on the practicalities of how and where, in a process, sources of risk can be found and risk controlled.
- It provides risk control throughout a process rather than relying on final product inspection.
- It draws attention to risk introduced through human actions and how this can be controlled at the point of introduction or subsequently.

Limitations include the following.

- HACCP requires that hazards are identified, the risks they represent defined, and their significance understood as inputs to the process. Appropriate controls also need to be defined. HACCP might need to be combined with other tools to provide these inputs.
- Taking action only when control parameters exceed defined limits can miss gradual changes in control parameters which are statistically significant and hence should be actioned.

B.4.3.6 Reference documents

[34] ISO 22000, *Food safety management systems – Requirements for any organization in the food chain*

[35] *Food Quality and Safety Systems – A Training Manual on Food Hygiene and the Hazard Analysis and Critical Control Point (HACCP) System*

B.4.4 Layers of protection analysis (LOPA)

B.4.4.1 Overview

LOPA analyses the reduction in risk that is achieved by set of controls. It can be considered as a particular case of an event tree (B.5.6) and is sometimes carried out as a follow up to a HAZOP study (B.2.4).

A cause-consequence pair is selected from a list of identified risks and the independent protection layers (IPLs) are identified. An IPL is a device, system or action that is capable of preventing a scenario from proceeding to its undesired consequence. Each IPL should be independent of the causal event or of any other layer of protection associated with the scenario and should be auditable. IPLs include:

- design features;
- physical protection devices;
- interlocks and shutdown systems;
- critical alarms and manual intervention;
- post event physical protection;
- emergency response systems.

Standard procedures and/or inspections do not directly add barriers to failure so in general should not be considered to be IPLs. The probability of failure of each IPL is estimated and an order of magnitude calculation is carried out to determine whether the overall protection is adequate to reduce risk to a tolerable level.

The frequency of occurrence of the undesired consequence can be found by combining the frequency of the initiating cause with the probabilities of failure of each IPL, taking into account any conditional modifiers. (An example of a conditional modifier is whether a person will be

present and might be influenced.) Orders of magnitude are used for frequencies and probabilities.

B.4.4.2 Use

LOPA can be used qualitatively to review the layers of protection between a causal factor and a consequence. It can also be used quantitatively to allocate resources to treatments by analysing the risk reduction produced by each layer of protection. It can be applied to systems with a long- or short-term time horizon and is usually used in dealing with operational risks.

LOPA can also be used quantitatively for the specification of IPLs and safety integrity levels (SIL levels) for instrumented systems, as described in IEC 61508 (all parts) and in IEC 61511 (all parts), and to demonstrate that a specified SIL is achieved.

NOTE An SIL is a discrete level (one out of a possible four) for specifying the reliability required of a safety-related system. Level 4 has the highest level of safety integrity and level 1 has the lowest.

B.4.4.3 Inputs

Inputs to LOPA include:

- basic information about sources, causes and consequences of events;
- information on controls in place or proposed treatments;
- the frequency of the causal event, and the probabilities of failure of the protection layers, measures of consequence and a definition of tolerable risk.

B.4.4.4 Outputs

The outputs are recommendations for any further treatments and estimates of the residual risk.

B.4.4.5 Strengths and limitations

Strengths of LOPA include the following.

- It requires less time and resources than event tree analysis or fully quantitative risk assessment but is more rigorous than subjective qualitative judgments.
- It helps identify and focus resources on the most critical layers of protection.
- It identifies operations, systems and processes for which there are insufficient safeguards.
- It focuses on the most serious consequences.

Limitations of LOPA include the following.

- It focuses on one cause-consequence pair and one scenario at a time; complex interactions between risks or between controls are not covered.
- When used quantitatively it might not account for common mode failures.
- It does not apply to very complex scenarios where there are many cause-consequence pairs or where there are a variety of consequences affecting different stakeholders.

B.4.4.6 Reference documents

- [36] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*
- [37] IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*
- [38] *Layer of protection analysis – Simplified process risk assessment*

B.5 Techniques for understanding consequences and likelihood

B.5.1 General

Techniques described in Clause B.5 aim to provide a greater understanding of consequences and their likelihood. In general the consequences can be explored by:

- experimentation, such as cell studies to explore consequences of exposure to toxins with results applied to human and ecological health risks;
- research into past events, including epidemiological studies;
- modelling to determine the way in which consequences develop following some trigger, and how this depends on the controls in place. This can include mathematical or engineering models and logic methods such as event tree analysis (B.5.6);
- techniques to encourage imaginative thinking such as scenario analysis (B.2.5).

The likelihood of an event or of a particular consequence can be estimated by:

- extrapolation from historical data (provided there is sufficient relevant historical data for the analysis to be statistically valid). This especially applies for zero occurrences, when one cannot assume that because an event or consequence has not occurred in the past it will not occur in the near future;
- synthesis from data relating to failure or success rates of components of the systems: using techniques such as event tree analysis (B.5.6), fault tree analysis (B.5.7) or cause-consequence analysis (B.5.5);
- simulation techniques, to generate, for example, the probability of equipment and structural failures due to ageing and other degradation processes.

Experts can be asked to express their opinion on likelihoods and consequences, taking into account relevant information and historical data. There are a number of formal methods for eliciting expert judgement that make the use of judgment visible and explicit (see Clause B.1).

Consequence and likelihood can be combined to give a level of risk. This can be used to evaluate the significance of a risk by comparing the level of risk with a criterion for acceptability, or to put risks in a rank order.

Techniques for combining qualitative values of consequence and likelihood include index methods (B.8.6) and consequence/likelihood matrices (B.10.3). A single measure of risk can also be produced from a probability distribution of consequences (see for example VaR (B.7.2) and CVaR (B.7.3) and S-curves (B.10.4)).

B.5.2 Bayesian analysis

B.5.2.1 Overview

It is common to encounter problems where there is both data and subjective information. Bayesian analysis enables both types of information to be used in making decisions. Bayesian analysis is based on a theorem attributed to Reverend Thomas Bayes (1760). At its simplest, Bayes' theorem provides a probabilistic basis for changing one's opinion in the light of new evidence. It is generally expressed as in Formula (1):

$$\Pr(A|B) = \frac{\Pr(B|A)\Pr(A)}{\Pr(B)} \quad (1)$$

where

$\Pr(A)$ is the prior assessment of the probability of A ;

$\Pr(B)$ is the prior assessment of the probability of B ;

$\Pr(A|B)$ is the probability of A given that B has occurred (the posterior assessment);

$\Pr(B|A)$ is the probability of B given A has occurred.

Bayes' theorem can be extended to encompass multiple events in a particular sample space.

For example, assume we have some data, D , that we wish to use to update our previous understanding (or lack thereof) of risk. We want to use these data to assess the relative merits of a number (N) of competing and non-overlapping hypotheses, which we will denote by H_n (where $n = 1, 2, \dots, N$). Then Bayes' theorem can be used to calculate the probability of the j th hypothesis using Formula (2):

$$\Pr(H_j | D) = \Pr(H_j) \left[\frac{\Pr(D | H_j)}{\sum \Pr(H_n) \Pr(D | H_n)} \right] \quad (2)$$

where $j = 1, 2, \dots, n$.

This shows that once the new data is accounted for, the updated probability for hypothesis j [i.e. $\Pr(H_j|D)$] is obtained by multiplying its prior probability $\Pr(H_j)$ by the bracketed fraction.

This fraction's numerator is the probability of getting these data if the j th hypothesis is true. The denominator comes from the "law of total probability" – the probability of getting these data if, one by one, each hypothesis were to be true. The denominator is the normalization factor.

A Bayesian probability can be more easily understood if it is considered as a person's degree of belief in a certain event as opposed to the classical probability which is based upon physical evidence.

B.5.2.2 Use

Bayesian analysis is a means of inference from data, both judgemental and empirical. Bayesian methods can be developed to provide inference for parameters within a risk model developed for a particular context; for example, the probability of an event, the rate of an event, or the time to an event.

Bayesian methods can be used to provide a prior estimate of a parameter of interest based upon subjective beliefs. A prior probability distribution is usually associated with subjective data since it represents uncertainties in the state of knowledge. A prior can be constructed using subjective data only or using relevant data from similar situations. A prior estimate can provide a probabilistic prediction of the likelihood of an event and be useful for risk assessment for which there is no empirical data.

Observed event data can then be combined with the prior distribution through a Bayesian analysis to provide a posterior estimate of the risk parameter of interest.

Bayes' theorem is used to incorporate new evidence into prior beliefs to form an updated estimate.

Bayesian analysis can provide both point and interval estimates for a parameter of interest. These estimates capture uncertainties associated with both variability and the state of knowledge. This is unlike classical frequentist inference which represents the statistical random variation in the variable of interest.

The probability model underpinning a Bayesian analysis depends on the application. For example, a Poisson probability model might be used for events such as accidents, non-conformances or late deliveries, or a binomial probability model might be used for one-shot

items. Increasingly it is common to build a probability model to represent the causal relationships between variables in the form of a Bayesian network (B.5.3).

B.5.2.3 Inputs

The inputs to a Bayesian analysis are the judgemental and empirical data needed to structure and quantify the probability model.

B.5.2.4 Outputs

Like classical statistics, Bayesian analysis provides estimates, both single numbers and intervals, for the parameter of interest and can be applied to a wide range of outputs.

B.5.2.5 Strengths and limitations

Strengths are the following.

- Inferential statements are easy to understand.
- It provides a mechanism for using subjective beliefs about a problem.
- It provides a mechanism for combining prior beliefs with new data.

Limitations are the following.

- It can produce posterior distributions that are heavily dependent on the choice of the prior.
- Solving complex problems can involve high computational costs and be labour intensive.

B.5.2.6 Reference documents

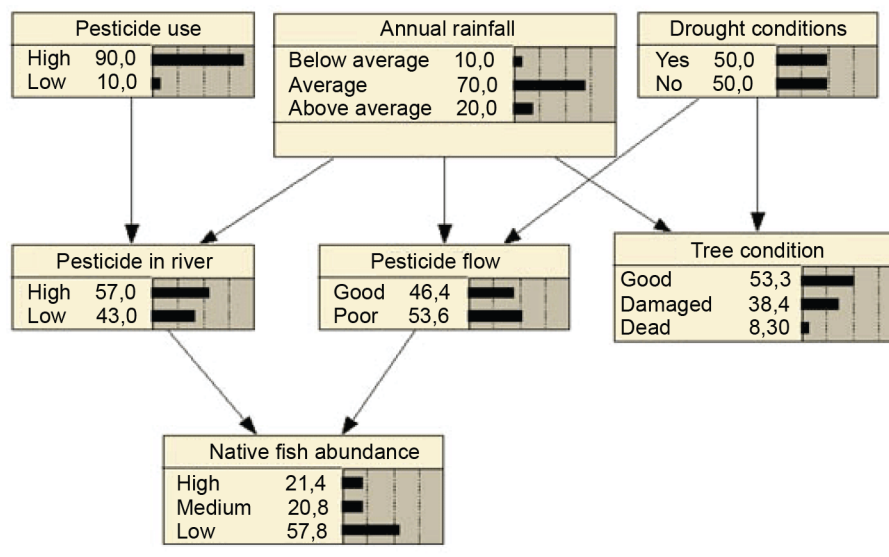
- [39] GHOSH, J., DELAMPADY, M. and SAMANTA, T. *An introduction to Bayesian analysis*, New York Springer-Verlag, 2006
- [40] QUIGLEY, J.L., BEDFORD, T.J. and WALLS, L.A. *Prior Distribution Elicitation*

B.5.3 Bayesian networks and influence diagrams

B.5.3.1 Overview

A Bayesian network (Bayes' net or BN) is a graphical model whose nodes represent the random variables (discrete and/or continuous) (Figure B.3). The nodes are connected by directed arcs that represent direct dependencies (which are often causal connections) between variables.

The nodes pointing to a node X are called its parents, and are denoted $pa(X)$. The relationship between variables is quantified by conditional probability distributions (CPDs) associated with each node, denoted $P(X|pa(X))$, where the state of the child nodes depends on the combination of the values of the parent nodes. In Figure B.3 probabilities are indicated by point estimates.



IEC

Figure B.3 – A Bayesian network showing a simplified version of a real ecological problem: modelling native fish populations in Victoria, Australia

B.5.3.2 Use

A basic BN contains variables that represent uncertain events and can be used to estimate likelihood or risk or to infer key risk drivers leading to specified consequences.

A BN can be extended to include decision actions and valuations as well as uncertainties, in which case it is known as an influence diagram, which can be used to assess the impact of risk controls/mitigations or to value intervention options.

A BN model can be built as a qualitative representation of a problem by stakeholders then quantified using relevant data, including judgemental (e.g. medicine distribution centre risk analysis), or a BN model can be learnt from empirical data only (e.g. web search engines, financial risk). Regardless of the form of a BN, the underlying inference mechanism is based on Bayes' theorem and possesses the general properties of Bayesian analysis (B.5.2).

BN have been used across a wide range of applications: including environmental decision making, medical diagnosis, critical infrastructure life extension, supply chain risk, new product and process development image modelling, genetics, speech recognition, economics, space exploration and in web search engines.

In general BNs provide visual models that support articulation of problems and communication between stakeholders. BN models allow sensitivity analysis to be conducted to explore "what if?" scenarios. Constructing the qualitative BN structure can be supported by the use of causal mapping (B.6.1) and a BN can be used in conjunction with scenario analysis (B.2.5) and cross impact analysis (B.6.2).

BNs are useful for gaining stakeholder input and agreement for decisions where there is high uncertainty and a divergence of stakeholder views. The representation is readily comprehensible although expertise is required to produce it.

BNs can be useful for mapping risk analyses for non-technical stakeholders, by promoting transparency of assumptions and process and by treating uncertainty in a way that is mathematically sound.

B.5.3.3 Inputs

The inputs for BNs require an understanding of system variables (nodes), the causal links between them (directed arcs) and the prior and conditional probabilities for these relationships.

In the case of an influence diagram, the valuations are also required (e.g. financial loss, injuries, etc.).

B.5.3.4 Outputs

BNs provide conditional and marginal distributions in a graphical output that is generally considered easy to interpret, at least compared with other, black box models. The BN model and the data can be readily modified to easily visualize relationships and explore the sensitivity of parameters to different inputs.

B.5.3.5 Strengths and limitations

Strengths of BNs include the following.

- There is readily available software that is relatively easy to use and understand.
- They have a transparent framework and are able to rapidly run scenarios and analyse sensitivity of output to different assumptions.
- They can include subjective beliefs about a problem, together with data.

Limitations include the following.

- Defining all interactions for complex systems is difficult, and can become computationally intractable when conditional probability tables become too large.
- BNs are often static and don't typically include feedback loops. However, the use of dynamic BNs is increasing.
- Setting parameters requires knowledge of many conditional probabilities which are generally provided by expert judgement. BNs can only provide answers based on these assumptions (a limitation that is common to other modelling techniques).
- The user can input errors but the output might still give a believable answer; checking extremes can help to locate errors.

B.5.3.6 Reference documents

- [41] NEIL, Martin and FENTON, Norman. *Risk Assessment and Decision Analysis with Bayesian Networks* CRC Press, 2012
- [42] JENSEN, F.V., NIELSEN T. D. *Bayesian Networks and Decision Graphs*, 2nd ed. Springer, New York, 2007
- [43] NICHOLSON, A., WOODBERRY O and TWARDY C, The "Native Fish" Bayesian networks. *Bayesian Intelligence Technical Report 2010/3*, 2010
- [44] NETICA TUTORIAL

B.5.4 Business impact analysis (BIA)

B.5.4.1 Overview

Business impact analysis analyses how incidents and events could affect an organization's operations, and identifies and quantifies the capabilities that would be needed to manage it. Specifically, a BIA provides an agreed understanding of:

- the criticality of key business processes, functions and associated resources and the key interdependencies that exist for an organization;
- how disruptive events will affect the capacity and capability of achieving critical business objectives;

- the capacity and capability needed to manage the impact of a disruption and recover to agreed levels of operation.

BIA can be undertaken using questionnaires, interviews, structured workshops or a combination of all three.

B.5.4.2 Use

BIA is used to determine the criticality and recovery time frames of processes and associated resources (e.g. people, equipment and information technology) to enable appropriate planning for disruptive events. BIA also assists in determining interdependencies and interrelationships between processes, internal and external parties and any supply chain linkages.

It can also be used as part of consequence analysis when considering consequences of disruptive events.

The BIA provides information that helps the organization determine and select appropriate business continuity strategies to enable effective response and recovery from a disruptive incident.

B.5.4.3 Inputs

Inputs include:

- information concerning the objectives, strategic direction, environment, assets, and interdependencies of the organization;
- overview of the organization's business products and services and their relationship to business processes;
- an assessment of priorities from previous management review;
- details of the activities and operations of the organization, including processes, resources, relationships with other organizations, supply chains, outsourced arrangements, and stakeholders;
- information to enable assessment of financial, legal and operational consequences of loss of critical processes;
- a prepared questionnaire or other means of collecting information;
- outputs of other risk assessment and critical incident analyses relating to outcomes of disruptive incidents;
- a list of people from relevant areas of the organization and/or stakeholders that will be contacted.

B.5.4.4 Outputs

The outputs include:

- a prioritized list of the organization's products and services;
- documents detailing the information collected as inputs;
- a prioritized list of critical processes and associated interdependencies;
- documented impacts from a loss of the critical processes including financial, legal, environmental and operational impacts;
- information on supporting resources and activities needed to re-establish critical processes;
- an assessment of the impacts over time of not delivering those products and services in the short, medium and long term;
- prioritized time frames for resuming delivery of those products and services at a specified minimum level, taking into account the time after which impacts of not resuming them would become unacceptable;

- outage time frames for the critical process and the associated information technology recovery time frames.

B.5.4.5 Strengths and limitations

Strengths of the BIA include that it provides:

- a deep understanding of the critical processes that enable an organization to achieve its objectives and which can indicate areas for business improvement;
- information needed to plan an organization's response to a disruptive event;
- an understanding of the key resources required in the event of a disruption;
- an opportunity to redefine the operational process of an organization to assist in improving the resilience of the organization.

Limitations include the following.

- BIA relies on the knowledge and perceptions of the participants involved in completing questionnaires, or in undertaking interviews or workshops. This can lead to simplistic or over-optimistic expectations of recovery requirements.
- Group dynamics can adversely affect the complete analysis of a critical process.
- There can be simplistic or over-optimistic expectations of recovery requirements.
- It can be difficult to obtain an adequate level of understanding of the organization's operations and activities.

B.5.4.6 Reference documents

[45] ISO TS 22317, *Societal security – Business continuity management systems – Guidelines for Business Impact Analysis*

[46] ISO 22301, *Societal security – Business continuity management systems – Requirements*

B.5.5 Cause-consequence analysis (CCA)

B.5.5.1 Overview

In some circumstances an event that could be analysed by a fault tree is better addressed by CCA. For example:

- if it is easier to develop event sequences than causal relationships;
- if the FTA might become very large;
- if there are separate teams dealing with different parts of the analysis.

In practice it is often not the top event that is defined first but potential events at the interface between the functional and technical domain.

For example, consider the event "loss of crew or vehicle" for a space craft mission. Rather than building a large fault tree based on this top event, intermediate undesired events such as ignition fails or thrust failure can be defined as top events and analysed as separate fault trees. These top events would then in turn be used as inputs to event trees to analyse operational consequences.

Two types of CCA can be distinguished, depending on which part of the analysis is more relevant to the circumstances. When detailed causes are required but a more general description of consequence is acceptable then the fault tree part of the analysis is expanded and the analysis is referred to as CCA-SELF (small event tree large fault tree). When a detailed description of consequence is required but cause can be considered in less detail, the analysis is referred to as CCA-LESF (large event tree small fault tree). Figure B.4 shows a conceptual diagram of a typical cause-consequence analysis.

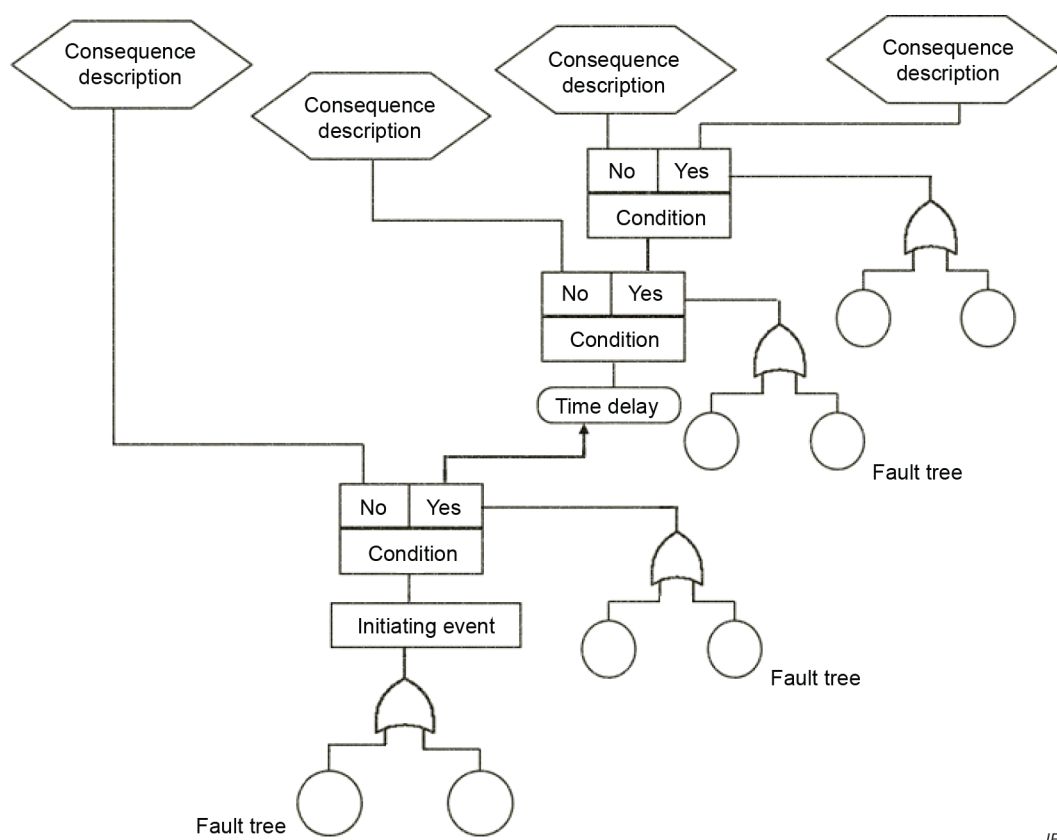
B.5.5.2 Use

Like fault tree analysis, CCA is used to represent the failure logic leading to a critical event but it adds to the functionality of a fault tree by allowing time sequential failures to be analysed. The method also allows time delays to be incorporated into the consequence analysis, which is not possible with event trees. It analyses the various paths a system could take following a critical event depending on the behaviour of particular subsystems (such as emergency response systems).

If quantified, a cause-consequence analysis will give an estimate of the probability of different possible consequences following a critical event.

As each sequence in a cause-consequence diagram is a combination of sub-fault trees, cause-consequence analysis can be used to build large fault trees.

Since the diagrams are complex to produce and use, the technique tends to be applied when the magnitude of the potential consequence of failure justifies intensive effort.



IEC

Figure B.4 – Example of cause-consequence diagram

B.5.5.3 Inputs

An understanding of the system and its failure modes and failure scenarios is required.

B.5.5.4 Outputs

The outputs of CCA are:

- a diagrammatic representation of how a system might fail showing both causes and consequences;

- an estimation of the probability of occurrence of each potential consequence based on analysis of probabilities of occurrence of particular conditions following the critical event.

B.5.5.5 Strengths and limitations

In addition to strengths of fault and event trees, CCA is better able to simultaneously represent the causes and consequences of a focus event and time dependencies than these techniques.

Limitations include that CCA is more complex than fault tree and event tree analysis, both to construct, and in the manner in which dependencies are dealt with during quantification.

B.5.5.6 Reference documents

- [47] ANDREWS J.D, RIDLEY L.M. 2002. Application of the cause-consequence diagram method to static systems
- [48] NIELSEN D.S. *The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis*

B.5.6 Event tree analysis (ETA)

B.5.6.1 Overview

ETA is a graphical technique that represents the mutually exclusive sequences of events that could arise following an initiating event according to whether the various systems designed to change the consequences function or not. The tree can be quantified to provide the probabilities of the different possible outcomes (see Figure B.5).

The tree starts with the initiating event then for each control lines are drawn to represent its success or failure. A probability of failure or success can be assigned to each control, by expert judgement, from data, or from individual fault tree analyses. The probabilities are conditional probabilities. For example, the probability of an item functioning is not the probability obtained from tests under normal conditions, but the probability of functioning under the conditions of the initiating event.

The frequency of the different outcomes is represented by the product of the individual conditional probabilities and the probability or frequency of the initiation event, given that the various events are independent. In Figure B.5 the probability of the initiating event is assumed to be 1.

B.5.6.2 Use

ETA can be used qualitatively to help analyse potential scenarios and sequences of events following an initiating event, and to explore how outcomes are affected by various controls. It can be applied at any level of an organization and to any type of initiating event.

Quantitative ETA can be used to consider the acceptability of the controls and the relative importance of different controls to the overall level of risk. Quantitative analysis requires that controls are either working or not (i.e. it cannot account for degraded controls) and that controls are independent. This is mostly the case for operational issues. ETA can be used to model initiating events which might bring loss or gain. However, circumstances where pathways to optimize gain are sought are more often modelled using a decision tree (B.9.3).

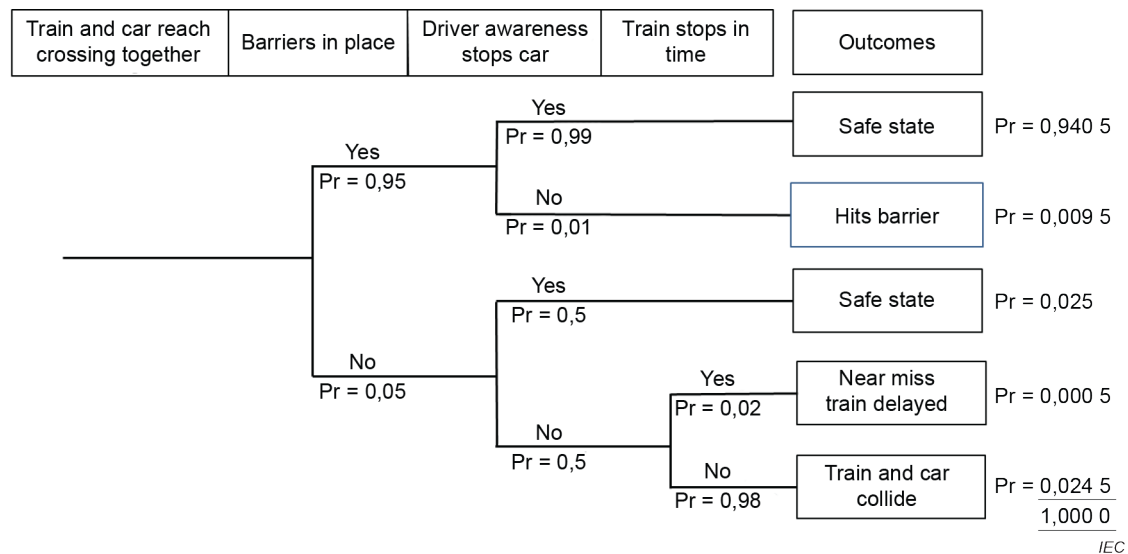


Figure B.5 – Example of event tree analysis

B.5.6.3 Inputs

Inputs include:

- a specified initiating event;
- information on barriers and controls, and, for quantitative analysis, their failure probabilities;
- an understanding of possible scenarios.

B.5.6.4 Outputs

Outputs from ETA include the following:

- qualitative descriptions of potential outcomes from initiating events;
- quantitative estimates of event rates/frequencies or probabilities and the relative importance of various failure sequences and contributing events;
- quantitative evaluations of effectiveness of controls.

B.5.6.5 Strengths and limitations

Strengths of ETA include the following.

- Potential scenarios following an initiating event are analysed and the influence of the success or failure of controls shown in a clear diagrammatic way that can, if required, be quantified.
- It identifies end events that might otherwise not be foreseen.
- It identifies potential single point failures, areas of system vulnerability and low payoff counter-measures, and hence can be used to improve control efficiency.
- The technique accounts for timing and for domino effects that are cumbersome to model in fault trees.

Limitations include the following.

- For a comprehensive analysis, all potential initiating events need to be identified. There is always a potential for missing some important initiating events or event sequences.
- Only success and failure states of a system are dealt with, and it is difficult to incorporate partially operating controls, delayed success or recovery events.

- Any path is conditional on the events that occurred at previous branch points along the path. Many dependencies along the possible paths are therefore addressed. However, some dependencies, such as common components, utility systems and operators, might be overlooked leading to optimistic estimations of the likelihood of particular consequences.
- For complex systems the event tree can be difficult to build from scratch.

B.5.6.6 Reference documents

[49] IEC 62502, *Analysis techniques for dependability – Event tree analysis*

[50] IEC TR 63039, *Probabilistic risk analysis of technological systems – Estimation of final event rate at a given initial state*

B.5.7 Fault tree analysis (FTA)

B.5.7.1 Overview

FTA is a technique for identifying and analysing factors that contribute to a specified undesired event (called the "top event"). The top event is analysed by first identifying its immediate and necessary causes. These could be hardware or software failures, human errors or any other pertinent events. The logical relationship between these causes is represented by a number of gates such as AND and OR gates. Each cause is then analysed step-wise in the same way until further analysis becomes unproductive. The result is represented pictorially in a tree diagram (see Figure B.6), which is the graphical representation of a Boolean equation.

B.5.7.2 Use

FTA is used primarily at operational level and for short- to medium-term issues. It is used qualitatively to identify potential causes and pathways to the top event, or quantitatively to calculate the probability of the top event. For quantitative analysis strict logic has to be followed. This means that the events at inputs of an AND gate have to be both necessary and sufficient to cause the event above and the events at an OR gate represent all possible causes of the event above, any one of which might be the sole cause. Techniques based on binary decision diagrams or Boolean algebra are then used to account duplicate failure modes.

FTA can be used during design, to select between different options, or during operation to identify how major failures can occur and the relative importance of different pathways to the top event.

Closely related techniques are the cause tree, which is used retrospectively to analyse events which have already occurred, and the success tree, where the top event is a success. The latter is used to study the causes of success in order to achieve future successes.

Probabilities tend to be higher in a success tree than a fault tree and when calculating the probability of the top event the possibility that events might not be mutually exclusive should be taken into account.

B.5.7.3 Inputs

Inputs for fault tree analysis are the following.

- An understanding of the system and the causes of failure or success is required, as well as a technical understanding of how the system behaves in different circumstances. Detailed diagrams are useful to aid the analysis;
- For quantitative analysis of a fault tree, data on failure rates, or the probability of being in a failed state, or the frequency of failures and where relevant repair/recovery rates, etc. are required for all base events.
- For complex situations, software and an understanding of probability theory and Boolean algebra are recommended so inputs to the software are made correctly.

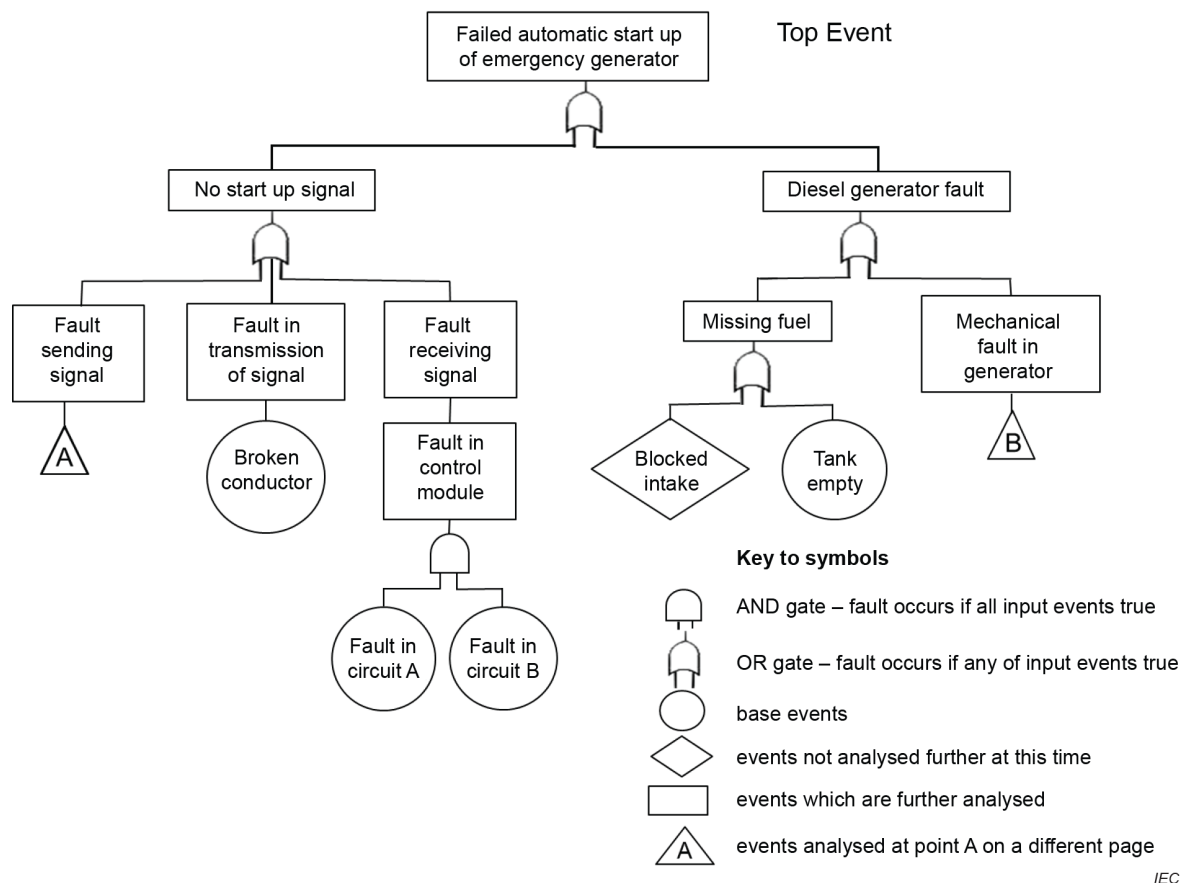


Figure B.6 – Example of fault tree

B.5.7.4 Outputs

The outputs from fault tree analysis are:

- a pictorial representation of how the top event can occur, which shows interacting pathways each of which involves the occurrence of two or more (base) events;
- a list of minimal cut sets (individual pathways to failure) with, provided data is available, the probability that each will occur;
- in the case of quantitative analysis, the probability of the top event and the relative importance of the base events.

B.5.7.5 Strengths and limitations

Strengths of FTA include the following.

- It is a disciplined approach which is highly systematic, but at the same time sufficiently flexible to allow analysis of a variety of factors, including human interactions and physical phenomena.
- It is especially useful for analysing systems with many interfaces and interactions.
- It provides a pictorial representation leading to an easier understanding of the system behaviour and the factors included.
- Logic analysis of the fault trees and the determination of cut sets is useful in identifying simple failure pathways in a complex system where particular combinations of events and event sequences which lead to the top event could be overlooked.
- It can be adapted to simple or complex problems with the level of effort dependent on complexity.

Limitations include the following.

- In some situations, it can be difficult to ascertain whether all important pathways to the top event are included; for example, including all ignition sources in an analysis of a fire. In these situations, it is not possible to calculate the probability of the top event.
- Time interdependencies are not addressed.
- FTA deals only with binary states (success/failure).
- While human error modes can be included in a fault tree, the nature and extent of such failures can be difficult to define.
- FTA analyses one top event. It does not analyse secondary or incidental failures.
- An FTA can get very large for large scale systems.

B.5.7.6 Reference documents

[51] IEC 61025, *Fault tree analysis (FTA)*

[16] IEC 62740, *Root cause analysis (RCA)*

B.5.8 Human reliability analysis (HRA)

B.5.8.1 Overview

HRA refers to a group of techniques that aim to evaluate a person's contribution to system reliability and safety by identifying and analysing the potential for an incorrect action. Although most often applied to degraded performance of operators in a safety context, similar methods can be applied to enhanced levels of performance. HRA is applied at a tactical level to particular tasks where correct performance is critical.

A hierarchical task analysis is first carried out to identify steps and sub-steps within an activity. Potential error mechanisms are identified for each substep often using a set of key-word prompts (such as too early, too late, wrong object, wrong action, right object).

Sources of these errors (such as distraction, time available too short, etc.) can be identified and the information used to reduce the likelihood of error within the task. Factors within the person themselves, the organization or the environment that influence the probability of error (performance shaping factors (PSFs)) are also identified.

The probability of an incorrect action can be estimated by various methods including using a data base of similar tasks or expert judgement. Typically, a nominal error rate for a task type is defined then a multiplier is applied to represent behavioural or environmental factors that increase or decrease the probability of failure. Various methods have been developed to apply these basic steps.

Early methods placed a strong emphasis on estimating the likelihood of failure. More recent qualitative methods focus on cognitive causes of variations in human performance with greater analysis of the way performance is modified by external factors and less on attempting to calculate a failure probability.

B.5.8.2 Use

Qualitative HRA can be used:

- during design so that systems are designed to minimize the probability of error by operators;
- during system modification to see whether human performance is likely to be influenced in either direction;
- to improve procedures so as to reduce errors;
- to assist in identifying and reducing error inducing factors within the environment or in organizational arrangements.

Quantitative HRA is used to provide data on human performance as input to logic tree methods or other risk assessment techniques.

B.5.8.3 Inputs

Inputs include:

- information to define tasks that people should perform;
- experience of the types of error or extraordinary performance that occur in practice;
- expertise on human performance and the factors which influence it;
- expertise in the technique(s) to be used.

B.5.8.4 Outputs

Outputs include:

- a list of errors or extraordinary performance that may occur and methods by which they can be enhanced through redesign of the system;
- human performance modes, types, causes and consequences;
- a qualitative or quantitative assessment of the risk posed by differences in performance.

B.5.8.5 Strengths and limitations

Strengths of HRA include the following.

- It provides a formal mechanism to include human performance when considering risks associated with systems where humans play an important role.
- Formal consideration of human performance modes and mechanisms based on an understanding of cognitive mechanisms can help identify ways modify the risk.

Limitations include the following.

- The methods are best suited to routine tasks carried out in well controlled environments. They are less useful for complex tasks or where actions must be based on multiple and possibly contradictory sources of information.
- Many activities do not have a simple pass/fail mode. HRA has difficulty dealing with partial impacts on performance as in the quality of actions or decisions.
- Quantification tends to be heavily reliant on expert opinion because little verified data is available.

B.5.8.6 Reference documents

[51] IEC 62508, *Guidance on human aspects of dependability*

[52] BELL Julie, HOLROYD Justin, *Review of human reliability assessment method*

[53] OECD, *Establishing the Appropriate Attributes in Current Human Reliability Assessment Techniques for Nuclear Safety*

B.5.9 Markov analysis

B.5.9.1 Overview

Markov analysis is a quantitative technique that can be applied to any system that can be described in terms of a set of discrete states and transitions between them, provided the evolution from its current state does not depend on its state at any time in the past.

It is usually assumed that transitions between states occur at specified intervals with corresponding transition probabilities (discrete time Markov chain). In practice this most commonly arises if the system is examined at regular intervals to determine its state. In some

applications the transitions are governed by exponentially distributed random times with corresponding transition rates (continuous-time Markov chain). This is commonly used for dependability analyses, see IEC 61165.

States and their transitions can be represented in a Markov diagram such as Figure B.7. Here the circles represent the states and the arrows represent the transitions between states and their associated transition probabilities. This example has only four states: good (S1), fair (S2), poor (S3) and failed (S4). It is assumed that each morning, the system is inspected and classified in one of these four states. If the system has failed, it is always repaired that day and returned to a good state.

The system can also be represented by a transition matrix as shown in Table B.4. Note that in this table the sum for each of the rows is 1 as the values represent the probabilities for all the possible transitions in each case.

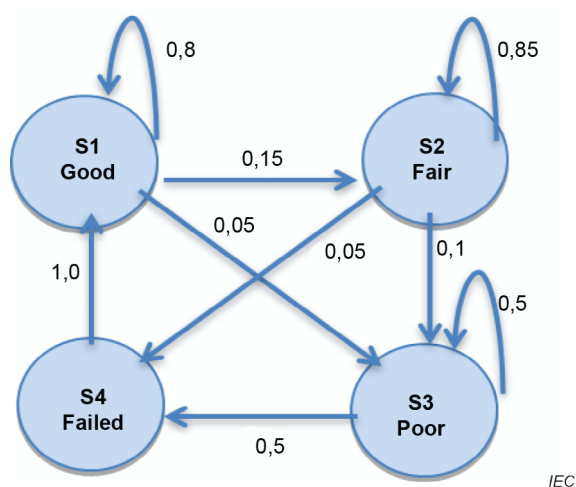


Figure B.7 – Example of Markov diagram

Table B.4 – Example of Markov matrix

		Next state after transition			
		S1, Good	S2, Fair	S3, Poor	S4, Failed
Current state	S1, Good	0,8	0,15	0,05	0
	S2, Fair	0	0,85	0,1	0,05
	S3, Poor	0	0	0,5	0,5
	S4, Failed	1	0	0	0

B.5.9.2 Use

Markov analysis can be used to estimate:

- the long-run probability of the system being in a specified state; for example, this might be the chance of a production machine operating as required, a component failing or a supply level falling below a critical threshold;
- the expected time to the first failure for a complex system (the first passage time), or the expected time before a system returns to a specified state (the recurrence time).

Examples of systems, states and transitions in different areas are provided in Table B.5.

Table B.5 – Examples of systems to which Markov analysis can be applied

Systems	States	Transitions
Technical systems	Condition of machines	Deterioration, breakdown, repair
Production	Production level	Operation, clean, reset
Marketing	Brand purchased	Brand loyalty, brand switching
Accounting	Accounts receivable status	Payment, write-off, extension
Health care	Patient status	Infection, recovery, treatment, relapse
Reservoir	Quantity of water	Inflows, outflows, evaporation
Human resources	Job categories	Movement between job categories and exit

B.5.9.3 Inputs

The inputs to a Markov analysis are a set of discrete states that the system can occupy, an understanding of the possible transitions that need to be modelled and estimates of the transition probabilities or transition rates (in the case of a continuous time Markov chain – CTMC).

B.5.9.4 Outputs

Markov analysis generates estimates of the probability of a system being in any specified state. It supports many kinds of decisions about the kinds of interventions a manager might make in a complex system (for example, to modify the states of the system and the transitions between them).

B.5.9.5 Strengths and limitations

Strengths of Markov analysis include the following.

- It can be used to model dynamic, multistate systems.
- State-transition diagrams provide simple and easily-communicated structures.

Limitations include the following.

- The assumptions might not apply to all systems of interest, in particular, the transition probabilities or transition rates between states can change through time as the system deteriorates or adapts.
- Accurate modelling can require extensive data collection and validation.
- Too much data reduces the answer to a mean.

B.5.9.6 Reference documents

[54] IEC 61165, *Application of Markov techniques*

[55] OXLEY, ALAN. *Markov Processes in Management Science*

B.5.10 Monte Carlo simulation

B.5.10.1 Overview

Some calculations carried out when analysing risk involve distributions. However, performing calculations with distributions is not easy as it is often not possible to derive analytical solutions unless the distributions have well-specified shapes, and then only with restrictions and assumptions that might not be realistic. In these circumstances, techniques such as Monte Carlo simulation provide a way of undertaking the calculations and developing results. Simulation usually involves taking random sample values from each of the input distributions, performing calculations to derive a result value, and then repeating the process through a series

of iterations to build up a distribution of the results. The result can be given as a probability distribution of the value or some statistic such as the mean value.

Systems can be developed using spreadsheets and other conventional tools, but more sophisticated software tools are available to assist with more complex requirements.

B.5.10.2 Use

In general, Monte Carlo simulation can be applied to any system for which:

- a set of inputs interact to define an output;
- the relationship between the inputs and outputs can be expressed as a set of dependencies;
- analytical techniques are not able to provide relevant results or when there is uncertainty in the input data.

Monte Carlo simulation can be used as part of risk assessment for two different purposes:

- uncertainty propagation on conventional analytical models;
- probabilistic calculations when analytical techniques don't work or are not feasible.

Applications include, amongst other things, modelling and the assessment of uncertainty in financial forecasts, investment performance, project cost and schedule forecasts, business process interruptions and staffing requirements.

B.5.10.3 Inputs

The inputs to a Monte Carlo simulation are:

- a model of the system that contains the relationship between different inputs, and between inputs and outputs;
- information on the types of inputs or the sources of uncertainty, that are to be represented;
- the form of output required.

Input data with uncertainty is represented as random variables with distributions which are more or less spread, according to the level of uncertainties. Uniform, triangular, normal and log normal distributions are often used for this purpose.

B.5.10.4 Outputs

The output could be a single value, or could be expressed as the probability or frequency distribution or it could be the identification of the main functions within the model that have the greatest impact on the output.

In general, the output of a Monte Carlo simulation will be either the entire distribution of outcomes that could arise, or key measures from a distribution such as:

- the probability of a defined outcome arising;
- the value of an outcome which the problem owners have a certain level of confidence will not be exceeded. Examples are a cost that there is less than a 10 % chance of exceeding or a duration that is 80 % certain to be exceeded.

An analysis of the relationships between inputs and outputs can throw light on the relative significance of the uncertainty in input values and identify targets for efforts to influence the uncertainty in the outcome.

B.5.10.5 Strengths and limitations

Strengths of Monte Carlo analysis include the following.

- The method can, in principle, accommodate any distribution in an input variable, including empirical data derived from observations of related systems.
- Models are relatively simple to develop and can be extended as the need arises.
- Any influences or relationships can be represented, including effects such as conditional dependencies.
- Sensitivity analysis can be applied to identify strong and weak influences;
- Models can be easily understood as the relationship between inputs and outputs is transparent.
- It provides a measure of the accuracy of a result.
- Software is readily available.

Limitations include the following.

- The accuracy of the solutions depends upon the number of simulations which can be performed.
- Use of the technique relies on being able to represent uncertainties in parameters by a valid distribution.
- It can be difficult to set up a model that adequately represents the situation.
- Large and complex models can be challenging to the modeller and make it difficult for stakeholders to engage with the process.
- The technique tends to de-emphasize high consequence/low probability risks.

Monte Carlo analysis prevents excessive weight being given to unlikely, high consequence, outcomes by recognizing that all such outcomes are unlikely to occur simultaneously across a portfolio of risks. This can have the effect of removing extreme events from consideration, particularly where a large portfolio is being considered. This can give unwarranted confidence to the decision maker.

B.5.10.6 Reference documents

[56] ISO/IEC Guide 98-3:2008/Suppl 1: *Uncertainty of measurement – Part 3: Guide to the expression of uncertainty in measurement (GUM 1995) – Propagation of distributions using a Monte Carlo method*

B.5.11 Privacy impact analysis (PIA) / data protection impact analysis (DPIA)

B.5.11.1 Overview

Privacy impact analysis (PIA) (also called privacy impact assessment) and data protection impact analysis (DPIA) methods analyse how incidents and events could affect a person's privacy (PI) and identify and quantify the capabilities that would be needed to manage it. A PIA/DPIA is a process for evaluating a proposal to identify the potential effects on individuals' privacy and personal data.

PIAs and DPIAs help organizations identify, assess and treat privacy risks associated with data processing activities. They are particularly important when a new data processing process, system or technology is being introduced. PIAs and DPIAs are an integral part of taking a privacy by design approach.

DPIAs also help organizations comply with the requirements of the data protection regulators (e.g. European Union General Data Protection Regulation, GDPR) and demonstrate that appropriate measures have been taken to ensure compliance.

Specifically, the process:

- analyses the potential consequences of a privacy infringement on a living person (basis risk screening);

- takes into account whether a processing of personal information has a high risk in case of a privacy incident;
- performs an in-depth risk analysis for processing of personal identifiable data.

A PIA/DPIA can be undertaken using questionnaires, interviews, structured workshops or a combination of all three, making use of the guidance of EU Article 29 Working Party and several templates developed by, for example, ICO (UK), CNIL (France), NOREA (NL).

B.5.11.2 Use

A PIA/DPIA is used to determine the consequences of high risks in processes and associated resources (e.g. people, equipment and information technology) to limit potential negative consequences on the privacy of people arising from the way information is treated.

It can also be used as part of consequence analysis when considering consequences of information processing more generally.

B.5.11.3 Inputs

Inputs include:

- information concerning the objectives, strategic direction, environment, assets, and interdependencies of the organization;
- an assessment of priorities from previous basic risk screening;
- details of the activities and operations of the organization when handling personal information, including processes, resources, relationships with other organizations, supply chains, outsourced arrangements, and stakeholders;
- information to enable assessment of financial, legal and operational consequences of a leak or loss of personal information (especially highly-sensitive personal information);
- a prepared questionnaire or other means of collecting information;
- outputs of other risk assessment and critical incident analyses relating to outcomes of relevant incidents (especially data leak or data loss incidents and other information security incidents which may have an effect on the intended data processing);
- a list of people from relevant areas of the organization and/or stakeholders that will be contacted.

B.5.11.4 Outputs

Outputs include:

- documents detailing the information collected as inputs;
- a prioritized list of critical information processes and associated interdependencies;
- a set of scenarios where risk is high for processing personal data as intended;
- documented impacts from a leak or loss of personal information on a living natural person;
- information on supporting resources and activities needed to limit potential consequences on data subjects;
- a prioritized list of the organization's products and services which are involved;
- an assessment of the impacts over time and means of not guaranteeing confidentiality, integrity and availability of (high-risk) personal data and consequences for the data subjects;
- outage time frames for the actions to be taken for containment and/or information recovery, declaration to the appropriate authorities and, in some cases, to the data subject(s).

B.5.11.5 Strengths and limitations

Strengths of the PIA/DPIA include that it provides:

- a deep understanding of the critical processes dealing with (sensitive) personal information within or on behalf of an organization;
- assessment of the implementation of privacy by design and by default principles;
- information needed to plan an organization's response to a personal data incident;
- an understanding of the key resources required in the event of a personal data leak or loss;
- an opportunity to redefine and reconsider the operational processing of personal data by an organization;
- in case of a legal obligation (e.g. European General Data Protection Regulation), documentation to inform data protection authorities before a high-risk processing of personal data begins.

Limitations include the following.

- There can be simplistic or underestimated calculation of the potential severity of risk for a person's privacy in the initial phase (privacy impact screening).
- PIA/DPIA relies on the knowledge and perceptions of the participants involved in completing questionnaires, or undertaking interviews or workshops.
- Group dynamics and time pressure can adversely affect the complete analysis of a critical process.
- It can be difficult to obtain an adequate level of understanding of the organization's operations and activities when processing personal data.

B.5.11.6 Reference documents

[57] EU: *General Data Protection Regulation* (European Union Official Journal, 04.05.2016)

[58] ICO (UK): *Data protection impact assessments*

[59] CNIL (FR), *Privacy Impact Assessment (PIA)*

B.6 Techniques for analysing dependencies and interactions

B.6.1 Causal mapping

B.6.1.1 Overview

Causal mapping captures individual perceptions in the form of chains of argument into a directed graph amenable for examination and analysis. Events, causes and consequences can be depicted in the map.

Typically, the maps are developed in a workshop environment where participants from a range of different disciplines are tasked with the elicitation, structuring and analysis of the material. Perceptions are augmented with information from documents where appropriate. Inputs can be captured using various tools ranging from sticky notes to specialized group decision support software. The latter allow for direct entry of issues and can be a highly productive means of working. The tools selected should allow for anonymous capture of issues so that an open and non-confrontational environment can be created to support focused discussion of causal relationships.

In general, the process starts by generating contributions that either impact or cause events in relation to the issue under consideration. These are then clustered according to their content and subsequently explored to ensure a comprehensive coverage.

Participants then consider how each of the events might impact upon one another. This enables the discrete events to be linked together to form causal reasoning paths in the map. The process aims to facilitate shared understanding of uncertain events as well as triggering further contributions through the enforced explanatory process, which is necessary for building up the chains of argument of how one event impacts another. There are clear rules for the capture of

both the nodes representing events and the relationships to ensure robust and comprehensive modelling.

Once the network of events has been developed to form a complete map, it can be analysed to determine properties that can be useful for managing risk: for example, to determine central nodes which are those events whose occurrence is central and can have substantial systemic effects; or to determine feedback loops, which can result in dynamic and destructive behaviours.

B.6.1.2 Use

Causal mapping identifies links and interactions between risks and themes within a list of risks.

It can be used forensically to develop a causal map for an event that has occurred (e.g. project overrun, system failure). Forensic causal maps can reveal triggers, consequences and dynamics. They allow for the determination of causality, which might be critical to claims.

Causal maps can also be used proactively to capture a comprehensive and systemic appreciation of event scenarios. The map can then be examined to allow deep learning as well as forming the basis for quantitative analysis of risks to help determine priorities.

They enable an integrated treatment programme to be developed rather than each risk being considered separately.

Causal analysis workshops can be run at regular intervals to ensure that the dynamic nature of risk is appreciated and managed appropriately.

B.6.1.3 Inputs

Data to inform the development of causal maps can come from a range of different sources such as from individual interviews where the maps produced give an in-depth representation of what occurred or could occur. Data can also be drawn from documentation such as reports, claim materials, etc. This data can be used directly or can be used to inform the process of analysing the chains of argument relating to events by participants in a workshop.

B.6.1.4 Outputs

The outputs include:

- causal maps which provide a visual representation of risk events and the systemic relationships between these events;
- the results of an analysis of the causal maps used to identify emergent clusters of events, critical events due to their centrality, feedback loops, etc.;
- a document translating the maps into text and reporting the key results, as well as explaining the selection of participants and the process used to develop the maps.

The outputs should provide information relevant to risk management decisions and an audit trail of the process used to generate this information.

B.6.1.5 Strengths and limitations

Strengths of causal maps include the following.

- The risks relevant to the issue under consideration are considered from the multiple perspectives of participants.
- The divergent and open nature of the process allows risk to be explored reducing the chance of overlooking critical events or relationships.
- The process allows the effective and efficient capture of the interactions between events and provides an understanding of their relationships.

- The process of determining the network of events that form the map can build the common language and understanding that are vital for effective risk management.

Limitations include the following.

- The process of mapping is not easy to learn as it demands not only skill in the mapping technique but also the ability to manage groups while working with the mapping tool.
- The maps are qualitative in nature and where quantification is required the maps need to be used as input to other appropriate models.
- The content of the map is determined by the sources and so careful consideration of participant make up is critical otherwise vital areas can be omitted.

B.6.1.6 Reference documents

- [60] BRYSON, J. M., ACKERMANN, F., EDEN, C., & FINN, C. *Visible thinking unlocking causal mapping for practical business results*
- [61] ACKERMANN, F, HOWICK, S, QUIGLEY, J, WALLS, L, HOUGHTON, T. *Systemic risk elicitation: Using causal maps to engage stakeholders and build a comprehensive view of risks*

B.6.2 Cross impact analysis

B.6.2.1 Overview

Cross impact analysis is the general name given to a family of techniques designed to evaluate changes in the probability of the occurrence of a given set of events consequent on the actual occurrence of one of them.

Cross impact analysis involves constructing a matrix to show the interdependencies of different events. A set of events or trends that might occur is listed along the rows, and the events or trends that would possibly be affected by the row events along the columns. Experts are then required to estimate:

- the probability for each event (in isolation of the others) at a given time horizon;
- the conditional probability of each event given that each other event occurs, i.e. for the i/j pair of events the experts estimate:
 - $P(i/j)$ – the probability of i if j occurs,
 - $P(i/\text{not } j)$ – the probability of i if j does not occur.

This is entered into a computer for analysis.

There are several different methods to calculate the probabilities of one event taking into account all other events. Regardless of how this is done, the usual procedure is to carry out a Monte Carlo simulation where the computer model systematically selects consistent sets of events and iterates a number of times. As more and more computer runs are performed, a new posterior probability of occurrence of each event is generated.

A sensitivity analysis is carried out by selecting an initial probability estimate or a conditional probability estimate, about which uncertainty exists. This judgment is changed and the matrix is run again.

B.6.2.2 Use

Cross impact analysis is used in forecasting studies and as an analytic technique to predict how different factors impact future decisions. It can be combined with scenario analysis (B.2.5) to decide which of the scenarios produced are the most likely. It can be used when there are multiple interacting risks, for example in complex projects, or in managing security risks.

The time horizon of cross impact analysis is usually medium to long term and can be from the present to five years or up to 50 years into the future. The time horizon should be explicitly stated.

The matrix of events and their interdependencies can be useful to decision makers as general background even without the probability calculated from the analysis.

B.6.2.3 Inputs

The method requires experts who are familiar with the issue under study, and have the capacity to envisage future developments, and who are able to estimate probabilities realistically.

Supporting software is needed to calculate the conditional probabilities. The technique requires specific modelling knowledge if the user wants to understand how the data are processed by the software. Significant time (several months) is usually required to develop and run the models.

B.6.2.4 Output

The output is a list of possible future scenarios and their interpretation. Each run of the model produces a synthetic future history, or scenario, which includes the occurrence of some events and the non-occurrence of others. On the basis of the specific cross impact model applied, the output scenarios attempt to generate either the most likely scenario, or a set of statistically consistent scenarios, or one or more plausible scenarios from the total set.

B.6.2.5 Strengths and limitations

Strengths of cross impact analysis include the following.

- it is relatively easy to implement a cross impact questionnaire.
- it forces attention into chains of causality (*a* affects *b*; *b* affects *c*, etc.).
- it can clarify and increase knowledge on future developments.
- it is useful in exploring a hypothesis and in finding points of agreement and divergence.

Limitations include the following.

- The number of events that can be included is limited in practice by both the software and the time required by experts. The number of runs required and the number of conditional probabilities to estimate increases rapidly as the number of events included increases (e.g. with a set of ten events an expert needs to provide 90 conditional probability judgments).
- A realistic study requires considerable work by experts and a high dropout rate is often experienced.
- It is difficult to define the events to be included and any influence not included in the set of events will be completely excluded from the study; conversely, the inclusion of irrelevant events can unnecessarily complicate the final analysis of the results.
- As with other techniques based on eliciting experts' knowledge, the method relies on the level of expertise of respondents.

B.6.2.6 Reference document

[62] JOINT RESEARCH CENTRE, EUROPEAN COMMISSION, *Cross impact analysis*, [viewed 2017-9-14]

B.7 Techniques that provide a measure of risk

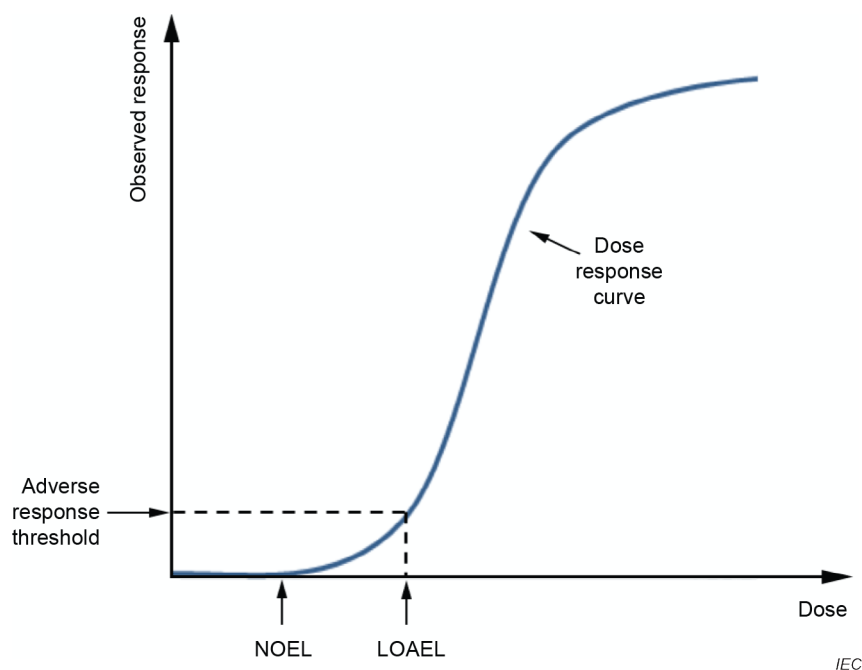
B.7.1 Toxicological risk assessment

B.7.1.1 Overview

Risk assessment in the context of risks to plants, animals, ecological domains, and humans as a result of exposure to a range of environmental hazards involves the following steps.

Risks to plants, animals, ecological domains, and humans can be due to physical, chemical and/or biological agents resulting in damage to DNA, birth defects, spread of disease, contamination of food chains and contamination of water. Assessment of such risks may require application of a range of techniques in the following steps.

- a) Problem formulation: This involves establishing the context of the assessment by defining the purpose of the assessment, the range of target populations and the hazard types of interest.
- b) Hazard identification and analysis: This involves identifying all possible sources of harm to the target population within the scope of the study and understanding the nature of the hazard and how it interacts with the target. For example, in considering human exposure to a chemical, the consequences considered could include the potential to damage DNA, or to cause cancer or birth defects. Hazard identification and analysis normally relies on expert knowledge and a review of literature.
- c) Dose response assessment: The response of the target population is usually a function of the level of exposure or dose. Dose response curves are usually developed from tests on animals, or from experimental systems such as tissue cultures. For hazards such as micro-organisms or introduced species, the dose response curve can be determined from field data and epidemiological studies. Wherever possible, the mechanism by which the effect is produced is determined. Figure B.8 shows a simplified dose response curve.



Key

NOEL	no observable effect limit
LOAEL	lowest observable adverse effect level

Figure B.8 – Example of dose response curve

- d) Exposure assessment: The dose that will be experienced in practice by the target population is estimated. This often involves a pathway analysis which considers the different routes the hazard might take, the barriers which might prevent it from reaching the target and the factors that might influence the level of exposure. For example, in assessing the risk from chemical spraying the exposure analysis would consider how much chemical was sprayed and under what conditions, whether there was any direct exposure of humans or animals, how much might be left as residue on plants, the environmental fate of any pesticide reaching the ground, whether it can accumulate in animals, whether it enters groundwater, etc.
- e) Risk characterization: The information from the previous steps is brought together to estimate the likelihood of particular consequences when effects from all pathways are combined.

B.7.1.2 Use

The method provides a measure for the magnitude of risk to human health or the environment. It is used in environmental impact statements to show whether the risk from a particular exposure is acceptable. It is also used as the basis for defining limits for acceptable risk.

B.7.1.3 Inputs

Inputs include information about the toxicological hazards, the ecological system of concern (including human health) and, where possible, the mechanisms involved. Typically, physical measurements are required to estimate exposures.

B.7.1.4 Outputs

The output is an estimate of the risk to human or ecological health, expressed either quantitatively or with a mixture of qualitative and quantitative information provided. The output may include limits to be used for defining acceptable limits for the hazard in the environment such as the no observable adverse effect limit (see Figure B.8).

B.7.1.5 Strengths and limitations

The strengths of this form of analysis include the following.

- It provides a very detailed understanding of the nature of the risk and the factors which increase risk.
- Pathway analysis is a very useful tool generally for all areas of risk to identify how and where it may be possible to improve controls or introduce new ones.
- The analysis can form the basis for simple rules about acceptable exposures that can be generally applied.

Limitations include the following.

- It requires good data which might not be immediately available. so significant research might be required.
- It requires a high level of expertise to apply.
- There is often a high level of uncertainty associated with dose response curves and the models used to develop them.
- Where the target is ecological rather than human and the hazard is not chemical, there might not be a good understanding of the systems involved.

B.7.1.6 Reference documents

[63] WORLD HEALTH ORGANISATION, *Human health risk assessment toolkit – chemical hazards*

[64] US EPA, *Guidelines for ecological risk assessment*

B.7.2 Value at risk (VaR)

B.7.2.1 Overview

Value at risk (VaR) is used widely in the financial sector to provide an indicator of the amount of possible loss in a portfolio of financial assets over a specific time period within a given confidence level. Losses greater than the VaR are suffered only with a specified small probability.

The distribution of profit and loss is usually derived in one of three ways.

- Monte Carlo simulation (see B.5.10) is used to model the drivers of variability in the portfolio and derive the distribution. This approach is particularly useful as it provides information about risks in the distribution tails, and it allows correlation assumptions to be tested.
- Historical simulation models make projections on the basis of looking back at observed outcomes and distributions. This is a simple approach, but it can be very misleading if future developments do not correspond with past experience, an important limitation in periods of market stress.
- Analytical methods are based on assumptions that the underlying market factors have a multivariate normal distribution. In this way, the profit and loss, which is also normally distributed, can be determined.

Many financial organizations use a combination of these approaches.

There is a requirement in some sectors for VaR to be calculated on the basis of stressed markets and conditions of high volatility to provide a credible set of "worst case" outcomes.

Common measures of VaR are related to losses over one-day and two-week horizons, with probabilities of loss of 1 % and 5 %. By convention, VaR is reported as a positive number, although it refers to a loss.

For example, Figure B.9 shows the distribution of value for a portfolio of financial assets over a period, with the distribution shown in cumulative form. Figure B.10 shows the region in which the portfolio suffers a loss, with VaR values of 1,6 million at 1 % (a probability of loss of 0,01) and 0,28 million at 5 % (a probability of loss of 0,05).

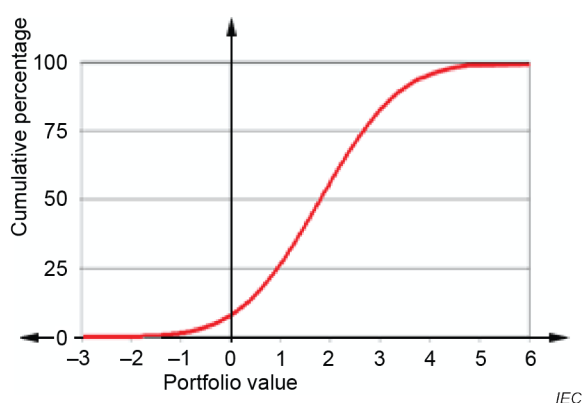


Figure B.9 – Distribution of value

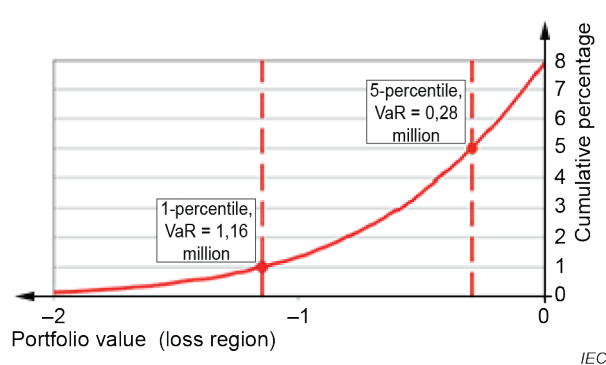


Figure B.10 – Detail of loss region VaR values

B.7.2.2 Use

VaR has three parameters: an amount of potential loss, the probability of that amount of loss, and the time period over which the loss might occur. It is used for the following purposes:

- to set limits for a portfolio manager on the maximum loss in the portfolio within an agreed risk tolerance or risk appetite;
- to monitor the "riskiness" of a portfolio of assets at a point in time and trends in riskiness;
- to determine how much economic, prudential or regulatory capital might need to be set aside for a specified portfolio;
- to report to regulators.

B.7.2.3 Inputs

The inputs are market factors that affect the value of the portfolio, such as exchange rates, interest rates and stock prices. Typically, these are identified by decomposing the instruments in the portfolio into simpler instruments directly related to basic market risk factors, then interpreting the actual instruments as portfolios of the simpler instruments. Funders and regulators can require specific methods to be adopted when assessing input variables.

B.7.2.4 Output

Over a nominated time period, VaR calculates the potential loss from a portfolio of financial assets for a specified probability. The analysis can also provide the probability for a specified amount of loss.

B.7.2.5 Strengths and limitations

Strengths include the following.

- The approach is straightforward, and accepted (or required) by financial regulators.
- It can be used to calculate economic capital requirements, on a daily basis if needed.
- It provides a means of setting limits on a trading portfolio in accordance with an agreed risk appetite, and monitoring performance against those limits, and so supporting governance.

Limitations include the following.

- VaR is an indicator not a specific estimate of possible loss. The maximum possible loss for any given situation is not evident from a single figure corresponding to VaR with 1 % or 5 % likelihood of loss derived from VaR analysis.
- VaR has a number of undesirable mathematical properties; for example, VaR is a coherent risk measure when based on an elliptical distribution such as the standard normal distribution but not in other circumstances. Calculations in the tail of the distribution are often unstable, and can depend on specific assumptions about distribution shapes and correlations that can be hard to justify and might not hold in times of market stress.
- Simulation models can be complex and time consuming to run.
- Organizations might require sophisticated IT systems to capture market information in a form that can be used easily, and in a timely manner, for VaR calculations.
- It is necessary to assume values for a set of parameters which are then fixed for the model. If the situation changes so these assumptions are not relevant the method will not give reasonable results. In other words, it is a risk model that cannot be used in unstable conditions.

B.7.2.6 Reference documents

- [65] CHANCE, D., BROOKS, R. (2010). *An introduction to derivatives and risk management*
- [66] THOMAS J. and PEARSON Neil D. Value at risk. *Financial Analysts Journal* 2000 **56**, 47-67

B.7.3 Conditional value at risk (CVaR) or expected shortfall (ES)

B.7.3.1 Overview

Conditional value at risk (CVaR), also called expected shortfall (ES), is a measure of the expected loss from a financial portfolio in the worst a % of cases. This is a similar measure to VaR, but it is more sensitive to the shape of the lower (loss) tail of the portfolio value distribution. $CVaR(a)$ is the expected loss from those losses that only occur a certain percentage of the time. For example in Figure B.10, when a is 5, then $CVaR(5)$ is the expected value of losses represented by the curve to the left of the vertical line at 5 %, i.e. the average of all losses greater than 0,28 million.

B.7.3.2 Use

CVaR techniques have been applied to credit risk measurement, which provides lenders with an insight into changes in extreme risk across industries since the onset of the financial crisis. Figure B.11 best illustrates the difference between CVaR and VaR in a portfolio at risk situation.

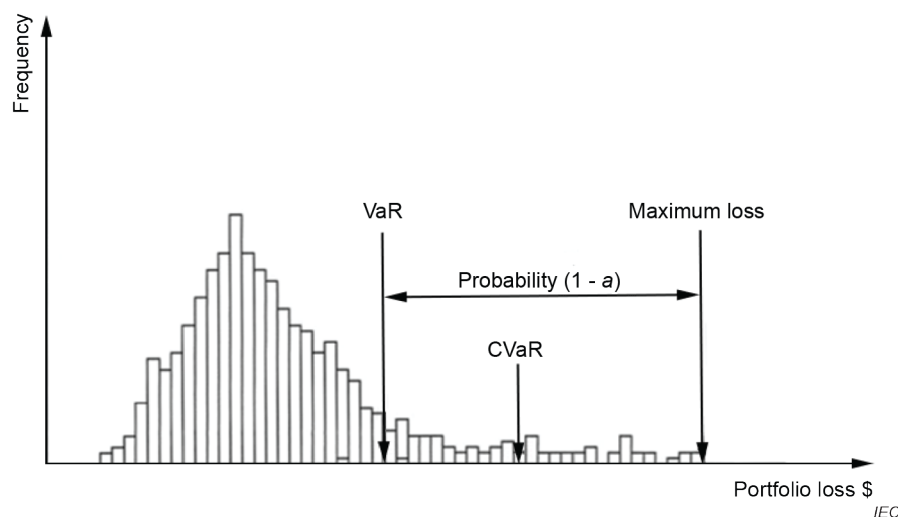


Figure B.11 – VaR and CVaR for possible loss portfolio

B.7.3.3 Inputs and outputs

See the description for value at risk (VaR) in B.7.2.

B.7.3.4 Strengths and limitations

Strengths include the following.

- CVaR is more sensitive to the shape of the distribution tail than VaR.
- CVaR avoids some of the mathematical limitations of VaR.
- CVaR is a more conservative measure than VaR because it focuses on the outcomes that generate the greatest losses.

Limitations include the following.

- CVaR is an indicator of potential for loss not an estimate of maximum possible loss;
- As with VaR, CVaR is sensitive to fundamental assumptions on volatility of asset value;
- CVaR relies on complex mathematics and requires a large range of assumptions.

B.7.3.5 Reference documents

[67] CHOUDHRY, M. *An introduction to Value at Risk*

[68] *Value at Risk*. New York University. [viewed 2017-9-14]. Available at: <http://people.stern.nyu.edu/adamodar/pdfiles/papers/VAR.pdf>

B.8 Techniques for evaluating the significance of risk

B.8.1 General

The techniques discussed in Clause B.8 are used within a process involving deciding whether and how to treat risk. Some can be used to decide whether a particular risk is tolerable or acceptable, others to indicate the relative significance of a risk or to rank risks in a priority order.

B.8.2 As low as reasonably practicable (ALARP) and so far as is reasonably practicable (SFAIRP)

B.8.2.1 Overview

ALARP and SFAIRP are acronyms that embody the principle of "reasonably practicable". They represent criteria where the test for acceptability or tolerability of a risk is whether it is reasonably practicable to do more to reduce risk. ALARP generally requires that the level of risk is reduced to as low as reasonably practicable. SFAIRP generally requires that safety is ensured so far as is reasonably practicable. Reasonably practicable has been defined in legislation or in case law in some countries.

The SFAIRP and ALARP criteria are intended to achieve the same outcome, however they differ on one semantic point. ALARP achieves safety by making risk as low as reasonably practicable, whereas SFAIRP makes no reference to the level of risk. SFAIRP is usually interpreted as a criterion by which controls are assessed to see if further treatments are possible; then, if they are possible, whether they are practicable. Both ALARP and SFAIRP make allowances for discounting risk treatments on the basis that the costs are grossly disproportionate to the benefits gained, although the extent to which this is available is jurisdiction dependent. For example, in some jurisdictions cost-benefit studies (see B.9.2) can be used to support an argument that ALARP or SFAIRP has been achieved.

The concept of ALARP, as originally expressed by the UK Health and Safety Executive, is illustrated in Figure B.12. In some jurisdictions quantified levels of risk are placed on the boundaries between intolerable, ALARP and broadly acceptable regions.

B.8.2.2 Use

ALARP and SFAIRP are used as criteria for deciding whether a risk needs to be treated. They are most commonly used for safety related risk and are used by legislators in some jurisdictions.

The ALARP model can be used to classify risks into one of three categories as follows:

- an intolerable risk category, where the risk cannot be justified except in extraordinary circumstances;
- a broadly acceptable risk category where the risk is so low that further risk reduction need not be considered (but could be implemented if practicable and reasonable);
- a region between these limits (the ALARP region) where further risk reduction should be implemented if it is reasonably practicable.

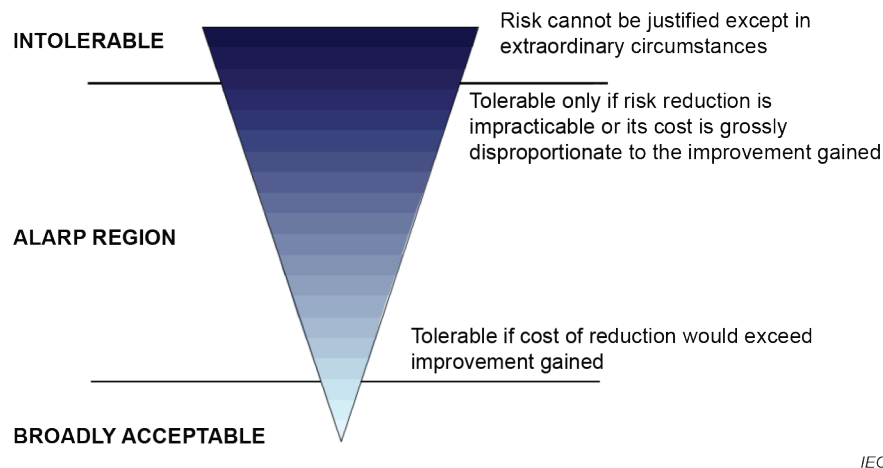


Figure B.12 – ALARP diagram

B.8.2.3 Inputs

Information about:

- the source of risk and the associated risk;
- criteria for limits to ALARP region;
- controls in place and what other controls would be possible;
- potential consequences;
- the likelihood those consequences would occur;
- the cost of possible treatments.

B.8.2.4 Output

The output is a decision about whether treatment is required and the treatment to be applied.

B.8.2.5 Strengths and limitations

The strengths of using the ALARP/SFAIRP criterion include that they:

- set a common standard of care, based on case law and legislation, that supports the principle of equity in that all individuals are entitled to an equal level of protection from risks which is deemed by law and not a variable deemed tolerable or acceptable by their organization;
- support the principle of utility as risk reduction should not require more effort than is reasonably practicable;
- allow for non-prescriptive goal setting;
- support continuous improvement towards the goal of minimizing risk;
- provide a transparent and objective methodology for discussing and determining acceptable or tolerable risk through stakeholder consultation.

Limitations include the following.

- Interpreting ALARP or SFAIRP can be challenging because it requires organizations to understand the legislative context of reasonably practicable and to exercise judgement with respect to that context.
- Applying ALARP or SFAIRP to new technologies can be problematic because risks and possible treatments might not be known or well understood.

- ALARP and SFAIRP set a common standard of care that may not be financially affordable for smaller organizations, resulting either in risk-taking or halting an activity.

B.8.2.6 Reference documents

- [69] HSE, 2010a, *HID'S Approach To 'As Low As Reasonably Practicable' (ALARP) Decisions*
- [70] HSE, 2010b, *Guidance on (ALARP) decisions in control of major accident hazards (COMAH)*
- [71] HSE, *Principles and guidelines to assist HSE in its judgments that duty-holders have reduced risk as low as reasonably practicable*

B.8.3 Frequency-number (F-N) diagrams

B.8.3.1 Overview

An F-N diagram is a special case of a quantitative consequence/likelihood matrix (B.10.3). In this application the X axis represents the cumulative number of fatalities and the Y axis the frequency with which they occur. Both scales are logarithmic to fit with typical data. The risk criteria are generally displayed as straight lines on the graph where the higher the slope of the line, the higher the aversion to a higher number of fatalities compared to a lower number.

B.8.3.2 Use

F-N diagrams are used either as a historical record of the outcome of incidents involving loss of human life, or to display the results of a quantitative analysis of the risk of loss of life in comparison with predefined criteria for acceptability.

Figure B.13 shows two examples of criteria labelled A and A-1 and B and B-1. They distinguish between an intolerable region (above A or B), a broadly acceptable region (below A-1 and B-1), and a region between the lines where the risks are acceptable if they are as low as reasonably practicable (ALARP) (B.8.2). The B criteria show both a higher slope (i.e. less tolerance for multiple fatalities) and more conservative limits overall. Also shown are six points on curve C, representing the results from a quantitative analysis of the level of risk to be compared with the criteria.

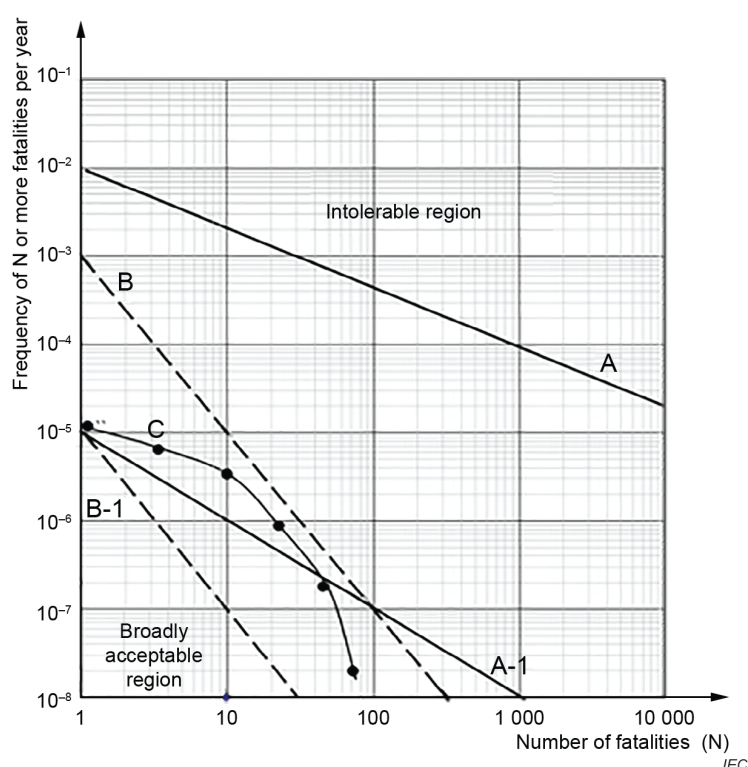


Figure B.13 – Sample F-N diagram

The most common application is for representing the societal risk from proposed major hazards sites that are subject to land use planning or similar safety evaluations.

NOTE Societal risk refers to societal concerns due to the occurrence of multiple fatalities in a single event.

B.8.3.3 Inputs

Data from incidents or from quantitative risk analysis that predicts the probability of fatalities.

B.8.3.4 Output

A graphical representation of the data compared with predefined criteria.

B.8.3.5 Strengths and limitations

The strengths of F-N diagrams include the following.

- They provide an easily understood output on which decisions can be based.
- The quantitative analysis necessary to develop an F-N plot provides a good understanding of the risk and its causes and consequences.

Limitations include the following.

- The calculations to produce the plots are often complex with many uncertainties.
- A full analysis requires all potential major accident scenarios to be analysed. This is time consuming and requires a high level of expertise.
- F-N diagrams cannot easily be compared with each other for the purpose of ranking (e.g. deciding which development provides the higher societal risk).

B.8.3.6 Reference documents

- [72] Understanding and using F-N Diagrams, *Annex in Guidelines for Developing Quantitative Safety Risk Criteria*
- [73] EVANS, A. *Transport fatal accidents and FN-curves*

B.8.4 Pareto charts

B.8.4.1 Overview

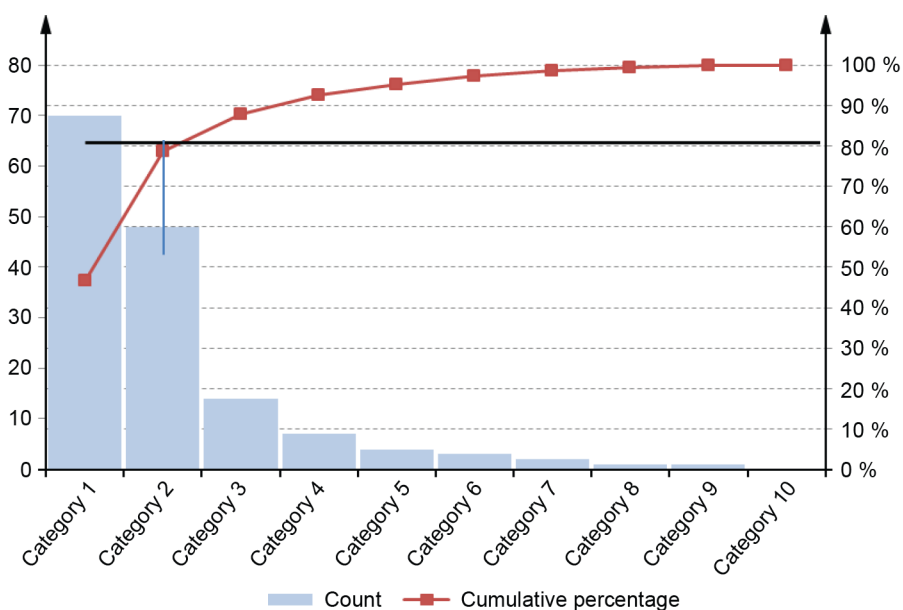
A Pareto chart (see Figure B.14) is a tool for selecting a limited number of tasks that will produce significant overall effect. It uses the Pareto principle (also known as the 80/20 rule), which is the idea that 80 % of problems are produced by 20 % of causes, or that by doing 20 % of the work one can generate 80 % of the benefit.

Producing a Pareto chart that selects causes to be addressed involves the following steps:

- identify and list problems;
- identify the cause of each problem;
- group problems together by cause;
- add up the scores for each group;
- draw a column graph with the causes displayed with those with the higher scores first.

The Pareto principle applies to the number of problems and takes no account of significance. In other words, high consequence problems may not be associated with the most common causes of lower consequence problems. This can be accommodated by scoring the problems according to consequence to provide a weighting. A Pareto analysis is a bottom-up approach and can deliver quantitative results. Although there is no sophisticated tool, or particular training or competence needed to apply this technique, some experience is very helpful to avoid common limitations and errors.

NOTE The figures 80 % and 20 % are illustrative – the Pareto principle illustrates the lack of symmetry that often appears between work put in and results achieved. For example, 13 % of work could generate 87 % of returns. Or 70 % of problems could be resolved by dealing with 30 % of the causes.



IEC

Figure B.14 – Example of a Pareto chart

B.8.4.2 Use

Pareto analysis is useful at an operational level when many possible courses of action are competing for attention. It can be applied whenever some form of prioritization is needed. For example, it can be used to help decide which causes are the most important to address or which risk treatments are the most beneficial.

A typical representation of a Pareto analysis is shown in the bar chart in which the horizontal axis represents categories of interest (e.g. material types, sizes, scrap codes, process centres), rather than a continuous scale (e.g. from 0 to 100). The categories are often "defects", sources of defects, or inputs into a process. The vertical axis represents some type of count or frequency (e.g., occurrences, incidents, parts, time). A line graph of the cumulative percentage is then drawn.

The categories to the left of where the cumulative percentage is intersected by the 80 % line are those that are dealt with.

B.8.4.3 Inputs

Data to analyse, such as data relating to past successes and failures and their causes.

B.8.4.4 Outputs

The output is a Pareto chart that helps demonstrate which categories are most significant, so that effort can be focused on areas where the largest improvements can be made. A Pareto chart can help visually determine which of the categories comprise the "vital few", and which represent the "trivial many". Although the analysis is quantitative, the output is a categorization of problems, causes, etc. ranked by importance.

If the first analysis contains many small or infrequent problems, they can be consolidated together into an "other" category. This is shown last on the Pareto chart (even if it is not the smallest bar). The cumulative percentage contribution line (the rolling sum of each category's contribution as a fraction of the total) can also be shown.

B.8.4.5 Strengths and limitations

Strengths of Pareto analysis include the following.

- Pareto analysis looks at the common causes of individual risks as a basis for a treatment plan.
- It provides a graphical output clearly indicating where the largest gains can be made.
- The time and effort needed to achieve results is likely to be moderate to low.

Limitations include the following.

- No account is taken of the cost or relative difficulty of dealing with each underlying cause.
- Data applicable to the situation being analysed need to be available.
- The data need to be able to be divided into categories and to fit the 80/20 rule for the method to be valid.
- It is difficult to construct relative weights when data is inadequate.
- Generally, only historical data are taken into consideration and there is no consideration of potential change.

B.8.4.6 Reference documents

[74] *Pareto Chart, Excel Easy*

[75] *Pareto Chart*

B.8.5 Reliability centred maintenance (RCM)

B.8.5.1 Overview

Reliability centred maintenance (RCM) is a risk-based assessment technique used to identify the appropriate maintenance policies and tasks for a system and its components so as to efficiently and effectively achieve the required safety, availability and economy of operation for all types of equipment. It encompasses all of the process steps to perform a risk assessment, including risk identification, risk analysis and risk evaluation.

The basic steps of an RCM programme are:

- initiation and planning;
- functional failure analysis;
- maintenance task selection;
- implementation;
- continuous improvement.

Functional analysis within RCM is most commonly carried out by performing a failure mode, effect and criticality analysis (FMECA, B.2.3), focusing on situations where potential failures can be eliminated or reduced in frequency and/or consequence by carrying out maintenance tasks. Consequences are established by defining failure effects then risk is analysed by estimating the frequency of each failure mode without maintenance being carried out. A risk matrix (B.10.3) allows categories for levels of risk to be established.

The appropriate failure management policy for each failure mode is then selected. Usually a standard task selection logic is applied to select the most appropriate tasks.

A plan is prepared to implement the recommended maintenance tasks by determining the detailed tasks, task intervals, procedures involved, required spare parts and other resources necessary to perform the maintenance tasks. An example is shown in Table B.6.

The entire RCM process is extensively documented for future reference and review. Collection of failure and maintenance-related data enables monitoring of results and implementation of improvements.

B.8.5.2 Use

RCM is used to enable applicable and effective maintenance to be performed. It is generally applied during the design and development phase of a system, then implemented during operation and maintenance. The greatest benefit is achieved by targeting the analysis on cases where failures would have serious safety, environmental, economic or operational effects.

RCM is initiated after a high-level criticality analysis identifies the system and equipment that requires maintenance tasks to be determined. This can occur either during the initial design phase, or later, during utilization, if it has not been done in a structured manner before or there is a need to review or improve maintenance.

B.8.5.3 Input

Successful application of RCM needs a good understanding of the equipment and structure, the operational environment and the associated systems, subsystems and items of equipment, together with the possible failures, and the consequences of those failures.

The process requires a team with requisite knowledge and experience, controlled by a trained and experienced facilitator.

B.8.5.4 Output

The end result of working through the process is a judgment as to the necessity of performing a maintenance task or other action such as operational changes.

The output is appropriate failure management policies for each failure mode, such as condition monitoring, failure finding, schedule restoration, replacement based on an interval (such as calendar, running hours, or number of cycles) or run-to-failure. Other possible actions that can result from the analysis include redesign, changes to operating or maintenance procedures or additional training. An example is given in Table B.6.

A plan is prepared to implement the recommended maintenance tasks. This details tasks, task intervals, procedures involved, required spare parts and other resources necessary to perform the maintenance tasks.

Table B.6 – An example of RCM task selection

Functional failure – Fails to provide compressor protection and shutdown							
Equipment	Failure mode	Failure interval (hours)	Failure detection	Causes	Task type	Task description	Task interval in hours
Pressure transmitter – compressor oil pressure	Inaccurate output	80 000	Evident	Out of calibration	Time directed	Verify calibration	16 000
Vibration transducer – compressor vibration	Fails to provide proper output	40 000	Evident	Detector/sensor failure	Condition directed	Verify accuracy if change in vibration occurs	Continuous on control panel
Level switch – low compressor oil level	Fails to change state on demand	80 000	Hidden	Detector/sensor failure	Failure finding	Functional test of level switch	8 000
Sensor and wiring – compressor oil temperature	Output high	160 000	Evident	Open circuit	Time directed	Check for loose connections	8 000
Level transmitter – glycol tank	Inaccurate output	40 000	Hidden	Out of calibration	Time directed	Calibrate transmitter preceded by confirmation of glycol fill level	8 000
Pressure transmitter – compressor suction/discharge pressure	Inaccurate output	80 000	Evident	Out of calibration	Time directed	Verify calibration	16 000
Sensor and wiring – compressor suction/discharge temperature	Output high	160 000	Evident	Open circuit	Time directed	Check for loose connections	8 000
Vibration transducer – cooler vibration	Fails to provide proper output	40 000	Evident	Detector/sensor failure	Condition directed	Verify accuracy if change in vibration occurs	Continuous on control panel

B.8.5.5 Strengths and limitations

Strengths include the following.

- The process enables magnitude of risk to be used to make maintenance decisions.
- Tasks are based on whether they are applicable, i.e. whether they will achieve the expected outcome.
- Tasks are evaluated to ensure they will be cost effective and worthwhile implementing.
- Unnecessary maintenance actions are eliminated with proper justification.
- The process and decisions are documented for later review.

Limitations include the following.

- The process is generally time consuming if it is to be effective.
- The process is very dependent on a trained and experienced facilitator.
- The team must have all of the necessary expertise and maintenance experience for the decisions to be valid.
- There may be a tendency to take shortcuts with the process, with impact on the validity of decisions being made.
- Potential tasks being considered will be limited by knowledge of available techniques such as those for condition monitoring.

B.8.5.6 Reference document

[76] IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

B.8.6 Risk indices

B.8.6.1 Overview

Risk indices provide a measure of risk which is derived using a scoring approach and ordinal scales. Factors which are believed to influence the magnitude of risk are identified, scored and combined using an equation that attempts to represent the relationship between them. In the simplest formulations, factors that increase the level of risk are multiplied together and divided by those that decrease the level of risk. Where possible the scales and the way they are combined are based on evidence and data.

It is important that the scores for each part of the system are internally consistent and maintain their correct relationships.

Mathematical formulae cannot be applied to ordinal scales. Therefore, once the scoring system has been developed, the model should be validated by applying it to a system that is well understood.

Developing an index is an iterative approach and several different systems for combining the scores should be tried to validate the method.

B.8.6.2 Use

Risk indices are essentially a qualitative or semi-quantitative approach to rank and compare risks. They can be used for internal or external risks of limited or extended scope. They are often specific to a particular type of risk and used to compare different situations where that risk occurs. While numbers are used, this is simply to allow for manipulation. In cases where the underlying model or system is not well known or not able to be represented, it is usually better to use a more overtly qualitative approach which does not imply a level of accuracy which is impossible using ordinal scales.

EXAMPLE 1 A disease risk index is used to estimate an individual's risk of contracting a particular disease by combining scores for various known risk factors identified in epidemiological studies, taking into account the strength of association between the risk factor and the disease.

EXAMPLE 2 Bush fire hazard ratings compare fire risk on different days taking account of predicted conditions such as humidity, wind strength, the dryness of the landscape and the fuel load.

EXAMPLE 3 Lenders calculate the credit risks for customers using indices that represent components of their financial stability.

B.8.6.3 Inputs

The inputs are derived from analysis of the system. This requires a good understanding of all the sources of risk, and how consequences can arise.

Tools such as FTA (B.5.7), ETA (B.5.6) and MCA (B.9.5) can be used as well as historical data to support the development of risk indices.

Since the choice of the ordinal scale used is, to some extent, arbitrary, sufficient data are needed to validate the index.

B.8.6.4 Output

The output is a series of numbers (composite indices) that relate to a particular risk and which can be compared with indices developed for other risks within the same system.

B.8.6.5 Strengths and limitations

Strengths of risk indices include the following.

- They can provide a simple easy to use tool for ranking different risks.
- They allow multiple factors which affect the level of risk to be incorporated into a single numerical score.

Limitations include the following.

- If the process (model) and its output are not well validated, the results can be meaningless.
- The fact that the output is a numerical value for risk can be misinterpreted and misused, for example in subsequent cost/benefit analysis.
- In many situations where indices are used, there is no fundamental model to define whether the individual scales for risk factors are linear, logarithmic or of some other form, and no model to define how factors should be combined. In these situations, the rating is inherently unreliable and validation against real data is particularly important.
- It is often difficult to obtain sufficient evidence to validate scales.
- The use of numerical values can imply a level of accuracy that cannot be justified.

B.8.6.6 Reference documents

[77] MACKENZIE Cameron A. *Summarizing risk using risk measures and risk indices*

B.9 Techniques for selecting between options

B.9.1 General

Techniques in Clause B.9 are used to help decision makers decide between options which involve multiple risks and where trade-offs have to be made. The techniques help to provide a logical basis to justify reasons for a decision. Since the methods have different philosophies, it can be valuable to explore options using more than one method.

Decision tree analysis and cost/benefit analysis base decisions on expected financial loss or gain. Multi-criteria analysis allows different criteria to be weighted and trade-offs made. Scenario analysis (see B.2.5) can also be used to explore the possible consequences if different options are followed. This method is particularly useful where there is high uncertainty. Decision problems can also be modelled using influence diagrams (B.5.3).

B.9.2 Cost/benefit analysis (CBA)

B.9.2.1 Overview

Cost/benefit analysis weighs the total expected costs of options in monetary terms against their total expected benefits in order to choose the most effective or the most profitable option. It can be qualitative or quantitative, or involve a combination of quantitative and qualitative elements, and can be applied at any level of an organization.

The stakeholders who might experience costs or receive benefits (tangible or intangible) are identified together with the direct and indirect benefits and costs to each.

NOTE Direct costs are those that are directly associated with the action. Indirect costs are those additional opportunity costs, such as loss of utility, distraction of management time or the diversion of capital away from other potential investments.

In quantitative CBA, a monetary value is assigned to all tangible and intangible costs and benefits. It often happens that the cost is incurred over a short period of time (e.g. a year) and the benefits flow for a long period. It is then necessary to discount the costs and benefits to bring them into "today's money" so that a valid comparison can be made between costs and benefits. The present value of all costs (PVC) and present value of benefits (PVB) to all stakeholders can be combined to produce a net present value (NPV): $NPV = PVB - PVC$.

A positive NPV implies that the action might be a suitable option. The option with the highest NPV is not necessarily the best value option. The highest ratio of NPV to the present value of costs is a useful indicator of the best value option. Selection based on CBA should be combined with strategic choice between satisfactory options which could individually offer lowest cost treatment, highest affordable benefit, or best value (most profitable return on investment). Such strategic choice can be required at both policy and operational level.

Uncertainty in costs and benefits can be taken into account by calculating the probability weighted average of net benefits (the expected net present value or ENPV). In this calculation the user is presumed to be indifferent between a small payoff with a high probability of occurrence, and a large payoff with a low probability of occurrence, so long as they both have the same expected value. NPV calculations can also be combined with decision trees (B.9.3) to model uncertainty in future decisions and their outcomes. In some situations it is possible to delay some of the costs until better information is available about costs and benefits. The possibility of doing this has a value which can be estimated using real options analysis.

In qualitative CBA no attempt is made to find a monetary value for intangible costs and benefits and, rather than providing a single figure summarizing the costs and benefits, relationships and trade-offs between different costs and benefits are considered qualitatively.

A related technique is a cost-effectiveness analysis. This assumes that a certain benefit or outcome is desired, and that there are several alternative ways to achieve it. The analysis looks only at costs and seeks to identify the cheapest way to achieve the benefit.

Although intangible values are usually dealt with by giving them a monetary value it is also possible to apply a weighting factor to other costs, for example to weight safety benefits more highly than financial benefits.

A variant of CBA – cost/benefit risk analysis (CBRA) – places greater emphasis on risk. Whereas CBA uses point or binary distributions, with CBRA the value for risk can also consider full probability distributions for negative and positive consequences [78].

B.9.2.2 Use

CBA is used at operational and strategic levels to help decide between options. In most situations those options will involve uncertainty. Both variability in the expected present value of costs, and benefits, and the possibility of unexpected events need to be taken into account in the calculations. A sensitivity analysis or Monte Carlo analysis (B.5.10) can be used for this.

CBA can also be used in making decisions about risks and their treatments, for example:

- as input into a decision about whether a risk should be treated;
- to decide on the best form of risk treatment;
- to compare long-term and short-term treatment options.

B.9.2.3 Inputs

Inputs include information on costs and benefits to relevant stakeholders and on uncertainties in those costs and benefits. Tangible and intangible costs and benefits should be considered. Costs include any resources which might be expended, including direct and indirect costs, attributable overheads and negative impacts. Benefits include positive impacts, and cost avoidance (which can result from risk treatments). Sunk costs already expended are not part of the analysis. A simple spreadsheet analysis or qualitative discussion does not require substantial effort, but application to more complex problems involves significant time in collecting necessary data and in estimating a suitable monetary value for intangibles.

B.9.2.4 Output

The output of a cost/benefit analysis is information on relative costs and benefits of different options or actions. This can be expressed quantitatively as a net present value (NPV), a best ratio (NPV/PVC) or as the ratio of the present value of benefits to the present value of costs.

A qualitative output is usually a table comparing costs and benefits of different types of cost and benefit, with attention drawn to trade-offs.

B.9.2.5 Strengths and limitations

Strengths of CBA include the following.

- CBA allows costs and benefits to be compared using a single metric (usually money).
- It provides transparency for information used to inform decisions.
- It encourages detailed information to be collected on all possible aspects of the decision (this can be valuable in revealing ignorance as well as communicating knowledge).

Limitations include the following.

- CBA requires a good understanding of likely benefits, so it does not suit a novel situation with high uncertainty.
- Quantitative CBA can yield dramatically different numbers, depending on the assumptions and methods used to assign economic values to non-economic and intangible benefits.
- In some applications it is difficult to define a valid discounting rate for future costs and benefits.
- Benefits which accrue to a large population are difficult to estimate, particularly those relating to the public good which is not exchanged in markets. However, when combined with "willingness to pay or accept", it is possible to account for such external or societal benefits.
- Depending on the discounting rate chosen, the practice of discounting to present values means that benefits gained in the long-term future can have negligible influence on the decision, so discouraging long-term investment.

- CBA does not deal well with uncertainty in the timing of when costs and benefits will occur or with flexibility in future decision making.

B.9.2.6 Reference documents

[79] *The Green book, Appraisal and Evaluation in Central Government*

[80] ANDOSEH, S., et al. *The case for a real options approach to ex-ante cost-benefit analyses of agricultural research projects*

B.9.3 Decision tree analysis

B.9.3.1 Overview

A decision tree models the possible pathways that follow from an initial decision that must be made (for example, whether to proceed with Project A or Project B). As the two hypothetical projects proceed, a range of events might occur and different predictable decisions will need to be made. These are represented in tree format, similar to an event tree. The probability of the events can be estimated together with the expected value or utility of the final outcome of each pathway.

Information concerning the best decision pathway is logically that which produces the best expected value calculated as the product of all the conditional probabilities along the pathway and the outcome value.

B.9.3.2 Use

A decision tree can be used to structure and solve sequential decision problems, and is especially beneficial when the complexity of the problem grows. It enables an organization to quantify the possible outcomes of decisions and hence helps decision makers select the best course of action when outcomes are uncertain. The graphical display can also help communicate reasons for decisions.

It is used to evaluate a proposed decision, often using subjective estimates of event probabilities, and helps decision makers to overcome inherent perception biases towards success or failure. It can be used on short-, medium- and long-term issues at an operational or strategic level.

B.9.3.3 Inputs

Developing a decision tree requires a project plan with decision points, information on possible outcomes of decisions and on chance events that might affect decisions. Expertise is needed to set up the tree correctly, particularly in complex situations.

Depending on the construction of the tree, quantitative data or sufficient information is needed to justify expert opinion for probabilities.

B.9.3.4 Outputs

Outputs include:

- a graphical representation of the decision problem;
- a calculation of the expected value for each possible path;
- a prioritized list of possible outcomes based on expected value, or the recommended pathway to be followed.

B.9.3.5 Strengths and limitations

Strengths of decision tree analysis include the following.

- It provides a clear graphical representation of the details of a decision problem.

- The exercise of developing the tree can lead to improved insights into the problem.
- It encourages clear thinking and planning.
- It enables a calculation of the best pathway through a situation and the expected result.

Limitations include the following.

- Large decision trees can become too complex for easy communication.
- There can be a tendency to oversimplify the situation so as to be able to represent it as a tree diagram.
- It relies on historical data which might not apply to the decision being modelled.
- It simplifies the decision problem outcomes discretizing it, which eliminates extreme values.

B.9.3.6 Reference document

[81] KIRKWOOD Craig, *Decision Tree Primer*

B.9.4 Game theory

B.9.4.1 Overview

B.9.4.1.1 General

Game theory is a means to model the consequences of different possible decisions given a number of possible future situations. The future situations can be determined by a different decision maker (e.g. a competitor) or by an external event, such as success or failure of a technology or a test. For example, assume the task is to determine the price of a product taking into account the different decisions that could be made by different decision makers (called players) at different times. The pay-off for each player involved in the game, relevant to the time period concerned, can be calculated and the strategy with the optimum payoff for each player selected. Game theory can also be used to determine the value of information about the other player or the different possible outcomes (e.g. success of a technology).

There are different types of games, for example cooperative/non-cooperative, symmetric/asymmetric, zero-sum/non-zero-sum, simultaneous/sequential, perfect information and imperfect information, combinatorial games, stochastic outcomes.

B.9.4.1.2 Communication and cooperative/non-cooperative games

An important factor is whether communication among players is possible or allowed. A game is cooperative if the players are able to form binding commitments. In non-cooperative games, this is not possible. Hybrid games contain cooperative and non-cooperative elements. For instance, coalitions of players are formed in a cooperative game, but these play in a non-cooperative fashion.

The classical example of games without communication between the players is the so called "prisoner's dilemma". It shows that in some cases the act of each player to improve their own outcome without regard for the other may cause the worst situation for both. This sort of game has been used to analyse conflict and cooperation between two players where lack of communication may cause an unstable situation that could result in the worst possible result for both players. In the prisoner's dilemma game, it is supposed that two persons committed a crime together. They are kept separate and cannot communicate. The police suggest a deal. If each prisoner will admit their guilt and testify against the other he will receive a low sentence, but the other prisoner will receive a larger sentence. A prisoner gets maximum penalty if he does not confess and testify and the other one does. Therefore to improve their situation both are tempted to confess and testify, but in that case they will both get the maximum penalty. Their best strategy would have been to reject the deal and not admit anything. In that case both would get the minimum penalty.

B.9.4.1.3 Zero-sum/non-zero-sum and symmetric/asymmetric games

In a zero-sum game, what one player gains, the other player loses. In a non-zero-sum game the sum of the outcomes may vary with the decisions. For example, lowering the prices may cost one player more than the other, but may increase the market volume for both.

B.9.4.1.4 Simultaneous/sequential games

In some games the calculation is made for just one interaction between the players. But in sequential games the players interact many times, and may change their strategy from one game to the next.

For example, simulated games have been made to investigate the effect of cheating in a market. There are two possibilities for each player. The supplier can deliver or not deliver, and the customer can pay or not pay. Of the four possible outcomes the normal outcome advantages both players (the supplier delivers and the customer pays). The outcome where the supplier does not deliver and the customer does not pay is a lost opportunity. The last two possibilities are a loss to the supplier (the customer does not pay) or to the customer (the supplier does not deliver). The simulation tried different strategies like always playing honest, always cheating or cheating at random. It was determined that the optimum strategy was to play honest in the first interaction and the next time to do what the other player did last time (play honest or cheat).

NOTE In real life it is likely that the supplier would recognize the customers that cheat and stop playing with them.

B.9.4.2 Use

Game theory allows risk to be evaluated in cases where the outcome of a number of decisions depends on the action of another player (e.g. a competitor) or on a number of possible outcomes (e.g. whether a new technology will work). The following example illustrates the information that can be achieved by a game analysis.

Table B.7 illustrates a situation where a company can choose between three different technologies. But the profit will depend on the action of a competitor (action 1, 2 or 3). It is not known what action the competitor will choose, but the probabilities are estimated as shown. The profits, in million monetary units (MU), are calculated in the table.

Table B.7 – Example of a game matrix

	Competitor			Expected profit	Guaranteed profit	Maximum regret
	Action 1	Action 2	Action 3			
Probability	0,4	0,5	0,1			
Technology 1	0,10	0,50	0,90	0,38	0,10	0,50
Technology 2	0,50	0,50	0,50	0,50	0,50	0,40
Technology 3	0,60	0,60	0,30	0,57	0,30	0,60

The following information can be extracted from the table to support the decision.

Clearly technology 3 is the best, with an expected profit of 0,57 million MU. But the sensitivity to the action of the competitor should be considered. The column guaranteed profit states what the profit will be for a given technology independent of what the competitor does. Here technology 2 is the best with a guaranteed profit of 0,50 million MU. It should be considered whether it is worth choosing technology 3 to gain only 0,07 million MU, risking the loss of 0,20 million MU.

It is further possible to compute the maximum regret, which is the difference between the profit from choosing a given technology and the profit possible had the action of the competitor been known. This gives the monetary benefit of increased knowledge of the competitor's decision.

This may be achieved by negotiation or by other legal means. In this example, the value of increased information is largest for technology 3.

B.9.4.3 Inputs

To be fully defined, a game must specify at least the following elements as inputs:

- the players or alternatives of the game;
- the information and actions available to each player at each decision point.

B.9.4.4 Output

The output is the payoff for each option in the game, generally taken to represent the utility of the individual players. Often in modelling situations the payoffs represent money, but other outcomes are possible (for example, market share or delay of a project).

B.9.4.5 Strengths and limitations

Strengths of game theory include the following.

- It develops a framework for analysing decision making where several decisions are possible, but where the outcome depends on the decision of another player or the outcome of a future event.
- It develops a framework for analysing decision making in situations where the interdependence of decisions made by different organizations is taken into account.
- It gives insights into several less-known concepts, which arise in situations of conflicting interest; for example, it describes and explains the phenomena of bargaining and coalition-formation.
- At least in zero-sum games in two organizations, game theory outlines a scientific quantitative technique that can be used by players to arrive at an optimal strategy.

Limitations include the following.

- It is assumed that players have knowledge about their own payoffs and the actions and pay offs of others might not be practical.
- The techniques of solving games involving mixed strategies (particularly in the case of a large pay-off matrix) are very complicated.
- Not all competitive problems can be analysed with the help of game theory.

B.9.4.6 Reference documents

[82] MYERSON, ROGER B., *Game Theory: Analysis of Conflict*

[83] MARYNARD, SMITH JOHN, *Evolution and Theory of Games*

[84] ROSENHEAD, J. and MINGER, J. (Eds), *Rational Analysis for a Problematic World Revisited*

B.9.5 Multi-criteria analysis (MCA)

B.9.5.1 Overview

MCA uses a range of criteria to transparently assess and compare the overall performance of a set of options. In general, the goal is to produce an order of preference for a set of options. The analysis involves the development of a matrix of options and criteria which are ranked and aggregated to provide an overall score for each option. These techniques are also known as multi-attribute (or multiple attribute) or multi-objective decision making. There are many variants of this technique, with many software applications to support them.

In general, an individual or a group of knowledgeable stakeholders undertakes the following process.

- Define the objective(s); determine the attributes (criteria or functional performance measures) that relate to each objective.
- Structure the attributes into a hierarchy of necessary and desirable requirements.
- Determine the importance of each criterion and assign weights to each.
- Gain stakeholder consensus on the weighted hierarchy.
- Evaluate the alternatives with respect to the criteria (this can be represented as a matrix of scores).
- Combine multiple single-attribute scores into an overall weighted multi attribute score.
- Evaluate the results for each option.
- Assess the robustness of the ranking of options by performing a sensitivity review to explore the impact of changing the attribute hierarchy weightings.

There are different methods by which the weighting for each criterion can be elicited and different ways of aggregating the criteria scores for each option into a single multi-attribute score. For example, scores can be aggregated as a weighted sum or a weighted product or using the analytic hierarchy process (an elicitation technique for the weights and scores based on pairwise comparisons). All these methods assume that the preference for any one criterion does not depend on the values of the other criteria. Where this assumption is not valid, different models are used.

Since scores are subjective, sensitivity analysis is useful to examine the extent to which the weights and scores influence overall preferences between options.

B.9.5.2 Use

MCA can be used for:

- comparing multiple options for a first pass analysis to determine preferred and inappropriate options;
- comparing options where there are multiple and sometimes conflicting criteria;
- reaching a consensus on a decision where different stakeholders have conflicting objectives or values.

B.9.5.3 Inputs

The inputs are a set of options for analysis and criteria, based on objectives, that can be used to assess the performance of options.

B.9.5.4 Outputs

The results can be presented as:

- rank order presentation of the options from best to least preferred;
- a matrix where the axes of the matrix are criteria weight and the criteria score for each option.

Presenting the results in a matrix allows options that fail highly weighted criteria or that fail to meet a necessary criterion to be eliminated.

B.9.5.5 Strengths and limitations

Strengths of MCA include that it can:

- provide a simple structure for efficient decision making and presentation of assumptions and conclusions;

- make more manageable complex decision problems, which are not amenable to cost/benefit analysis;
- help consider problems rationally where trade-offs need to be made;
- help achieve agreement when stakeholders have different objectives and hence different values and criteria.

Limitations include the following.

- MCA can be affected by bias and poor selection of the decision criteria.
- Aggregation algorithms which calculate criteria weights from stated preferences or aggregate differing views can obscure the true basis of the decision.
- The scoring system can oversimplify the decision problem.

B.9.5.6 Reference documents

- [85] EN 16271:2012, *Value management – Functional expression of the need and functional performance specification – Requirements for expressing and validating the need to be satisfied within the process of purchasing or obtaining a product*

NOTE EN 16271:2012 sets out approaches to reconcile conflicting stakeholder needs, methods which can be used to derive functional performance requirements, and guidance to set the granularity for multi-criteria analysis before comparing options.

- [86] DEPARTMENT FOR COMMUNITIES AND LOCAL GOVERNMENT, *Multi-criteria analysis: a manual* 2009

- [87] RABIHAH MHD.SUM (2001), *Risk Management Decision Making*

- [88] VELASQUEZ, M., HESTER, P. *An Analysis of Multi-criteria Decision Making Methods*

B.10 Techniques for recording and reporting

B.10.1 General

Clause B.10 covers techniques used for reporting and recording general information about risks. Requirements for detailed reports are covered in 6.6.

A common approach to reporting and recording information about risks is to enter basic information for each risk in a risk register such as a spreadsheet or data base (see B.10.2). Some risks can require a more complex description than can be accommodated in a traditional register of risks. For example, a description might need to include multiple sources of risk leading to a single event, multiple possible outcomes from a single event or source, knock-on effects and potential control failures. The bow tie diagram is an example of a tool which can be used to organize and communicate this sort of information (see B.4.2.)

Information about the magnitude of a risk can also be reported in a number of different ways. The most common method uses the consequence/likelihood matrix (see B.10.3). As well as the likelihood, consequence and level of risk, indicated by the position in the matrix, additional information such as the nature of controls, the extent to which treatments have been implemented, etc. can be provided through the size of the points marking the risk or their colour.

The consequence/likelihood matrix requires that a risk can be represented by a single consequence/likelihood pair. Risks, where this is not the case, can sometimes be represented by a probability distribution function or a cumulative distribution function (see B.10.4).

B.10.2 Risk registers

B.10.2.1 Overview

A risk register brings together information about risks to inform those exposed to risks and those who have responsibility for their management. It can be in paper or data base format and generally includes:

- a short description of the risk (e.g. a name, the consequences and sequence of events leading to consequences, etc.);
- a statement about the likelihood of consequences occurring;
- sources or causes of the risk;
- what is currently being done to control the risk.

Risks can be classified into different categories to aid reporting (B.2.2).

Risks are generally listed individually as separate events but interdependencies should be flagged.

In recording information about risks, the distinction between risks (the potential effects of what might happen) and risk sources (how or why it might happen) and controls that might fail should be explicit. It can also be useful to indicate the early warning signs that an event might be about to occur.

Many risk registers also include some rating of the significance of a risk, an indication of whether a risk is considered to be acceptable or tolerable, or whether further treatment is needed and the reasons for this decision. Where a significance rating is applied to a risk based on consequences and their likelihood, this should take account of the possibility that controls will fail. A level of risk should not be allocated for the failure of a control as if it were an independent risk.

Risks where consequences are positive can be recorded in the same document as those where consequences are negative or separately. Opportunities (which are circumstances or ideas that could be exploited rather than chance events) are generally recorded separately and analysed in a way that takes account of costs, benefits and any potential negative consequences. This can sometimes be referred to as a value and opportunities register.

B.10.2.2 Use

A risk register is used to record and track information about individual risks and how they are being controlled. It can be used to communicate information about risks to stakeholders and highlight particularly important risks. It can be used at corporate, departmental, operational and project level, where there are a large number of risks, controls and treatments that need to be tracked. Information from a risk register can be consolidated to provide information for top management.

A risk register can be used as the basis for tracking implementation of proposed treatments, so can contain information about treatments and how they will be implemented, or make reference to other documents or data bases with this information. (Such information can include risk owners, actions, action owners, action business case summaries, budgets and timelines, etc.). A form of risk register can be mandated in some situations.

B.10.2.3 Inputs

Inputs to a risk register are generally the outputs from risk assessment techniques such as described in Clauses B.1 to B.4, supplemented by records of failures.

B.10.2.4 Outputs

The outputs are records of information and reports about risks.

B.10.2.5 Strengths and limitations

Strengths of risk registers include the following.

- Information about risks is brought together in a form where actions required can be identified and tracked.
- Information about different risks is presented in a comparable format, which can be used to indicate priorities and is relatively easy to interrogate.
- The construction of a risk register usually involves many people and raises general awareness of the need to manage risk.

Limitations include the following.

- Risks captured in risk registers are typically based on events, which can make it difficult to accurately characterize some forms of risk (see 4.2).
- The apparent ease of use can give misplaced confidence in the information because it can be difficult to describe risks consistently and sources of risk, risks, and weaknesses in controls for risk are often confused.
- There are many different ways to describe a risk and any priority allocated will depend on the way the risk is described and the level of disaggregation of the issue.
- Considerable effort is required to keep a risk register up to date (for example, all proposed treatments should be listed as current controls once they are implemented, new risks should be continually added and those that no longer exist removed).
- Risks are typically captured in risk registers individually. This can make it difficult to consolidate information to develop an overall treatment programme.

B.10.2.6 Reference documents

There are no reference documents for this technique.

B.10.3 Consequence/likelihood matrix (risk matrix or heat map)

B.10.3.1 Overview

The consequence/likelihood matrix (also referred to as a risk matrix or heat map) is a way to display risks according to their consequence and likelihood and to combine these characteristics to display a rating for the significance of risk.

Customized scales for consequence and likelihood are defined for the axes of the matrix. The scales can have any number of points – three-, four- or five-point scales are most common – and can be qualitative, semi-quantitative or quantitative. If numerical descriptions are used to define the steps of the scales, they should be consistent with available data and units should be given. Generally, to be consistent with data, each scale point on the two scales will need to be an order of magnitude greater than the one before.

The consequence scale (or scales) can depict positive or negative consequences. Scales should be directly connected to the objectives of the organization, and should extend from the maximum credible consequence to the lowest consequence of interest. A part example for adverse consequences is shown in Figure B.15.

Rating	Financial	Health and safety	Environment and community	Etc.
a	Max credible loss (\$)	Multiple fatalities	Irreversible significant harm; community outrage	
b				
c				
d				
e	Minimum of interest (\$)	First aid only required	Minor temporary damage	

IEC

Figure B.15 – Part example of table defining consequence scales

NOTE Part examples are used so that the examples cannot be used directly to stress that the scales should always be customized.

Additional or fewer consequence categories may be used and the scales may have fewer or more than five points, depending on the context. The consequence rating column can be words, numbers or letters.

The likelihood scale should span the range relevant to data for the risks to be rated. A part example of a likelihood scale is shown in Figure B.16.

Rating	Descriptor	Descriptor meaning
5	Likely	Expected to occur within weeks
4		
3		
2		
1	Remotely possible	Theoretically possible but extremely unlikely

IEC

Figure B.16 – Part example of a likelihood scale

The likelihood rating scale may have more or less than five points and the ratings can be given as words, numerals or letters.

The likelihood scale should be tailored to the situation and may need to cover a different range for positive or negative consequences. If the highest consequence is deemed to be tolerable at some low likelihood then the lowest step on the likelihood scale should represent an acceptable likelihood for the highest defined consequence, (otherwise all activities with the highest consequence are defined as intolerable and cannot be made tolerable). In deciding the tolerable likelihood for a single, high consequence risk, the fact that multiple risks can lead to the same consequence should be taken into account.

A matrix is drawn with consequence on one axis and likelihood on the other corresponding to the defined scales. A rating for priority can be linked to each cell. In the example provided there

are five priority ratings, indicated here by Roman numerals. Typically, boxes are coloured to indicate the magnitude of risk. Decision rules (such as the level of management attention or the urgency of response) can be linked to the matrix cells. These will depend on the definitions used for the scales and the organization's attitude to risk. The design should enable the priority of a risk to be based on the extent to which the risk leads to outcomes that are outside the organization's defined performance thresholds for its objectives.

The matrix can be set up to give extra weight to consequences (as shown in Figure B.17) or to likelihood, or it can be symmetrical, depending on the application.

Consequence rating ↑	a	III	III	II	I	I
	b	IV	III	III	II	I
	c	V	IV	III	II	I
	d	V	V	IV	III	II
	e	V	V	IV	III	II
		1	2	3	4	5
						Likelihood rating →

IEC

Figure B.17 – Example of consequence/likelihood matrix

B.10.3.2 Use

A consequence/likelihood matrix is used to evaluate and communicate the relative magnitude of risks on the basis of a consequence/likelihood pair that is typically associated with a focal event.

To rate a risk, the user first finds the consequence descriptor that best fits the situation then defines the likelihood with which it is believed that consequence will occur. A point is placed in the box which combines these values, and the level of risk and associated decision rule are read off from the matrix.

Risks with potentially high consequences are often of greatest concern to decision makers even when the likelihood is very low, but a frequent but low impact risk can have large cumulative or long-term consequences. It can be necessary to analyse both kinds of risks as the relevant risk treatments can be quite different.

Where a range of different consequence values are possible from one event, the likelihood of any particular consequence will differ from the likelihood of the event that produces that consequence. Generally the likelihood of the specified consequence is used. The way that likelihood is interpreted and used should be consistent across all risks being compared.

The matrix can be used to compare risks with different types of potential consequence and has application at any level in an organization. It is commonly used as a screening tool when many risks have been identified, for example to define which risks need to be referred to a higher level of management. It can also be used to help determine if a given risk is broadly acceptable, or not acceptable according to the zone where it is located on the matrix. It can be used in situations where there is insufficient data for detailed analysis or the situation does not warrant the time and effort for a more detailed or quantitative analysis. A form of consequence/likelihood matrix can be used for criticality analysis in FMECA (B.2.3) or to set priorities following HAZOP (B.2.4) or SWIFT (B.2.6).

B.10.3.3 Inputs

A consequence/likelihood matrix needs to be developed to suit the context. This requires some data to be available in order to establish realistic scales. Draft matrices need to be tested to ensure that the actions suggested by the matrix match the organization's attitude to risk and that users correctly understand the application of the scales.

Use of the matrix needs people (ideally a team) with an understanding of the risks being rated and such data as is available to help in judgements of consequences and their likelihood.

B.10.3.4 Output

The output is a display which illustrates the relative consequence likelihood and level of risk for different risks and a significance rating for each risk.

B.10.3.5 Strengths and limitations

Strengths include the following.

- It is relatively easy to use.
- It provides a rapid ranking of risks into different significance levels.
- It provides a clear visual display of the relevant significance of risk by consequence, likelihood or level of risk.
- It can be used to compare risks with different types of consequence.

Limitations include the following.

- It requires good expertise to design a valid matrix.
- It can be difficult to define common scales that apply across a range of circumstances relevant to an organization.
- It is difficult to define the scales unambiguously to enable users to weight consequence and likelihood consistently.
- The validity of risk ratings depends on how well the scales were developed and calibrated.
- It requires a single indicative value for consequence to be defined, whereas in many situations a range of consequence values are possible and the ranking for the risk depends on which is chosen.
- A properly calibrated matrix will involve very low likelihood levels for many individual risks which are difficult to conceptualize.
- Its use is very subjective and different people often allocate very different ratings to the same risk. This leaves it open to manipulation.
- Risks cannot be directly aggregated (e.g. one cannot define whether a particular number of low risks, or a low risk identified a particular number of times, is equivalent to a medium risk).
- It is difficult to combine or compare the level of risk for different categories of consequences.
- A valid ranking requires a consistent formulation of risks (which is difficult to achieve).
- Each rating will depend on the way a risk is described and the level of detail given (i.e. the more detailed the identification, the higher the number of scenarios recorded, each with a lower likelihood). The way in which scenarios are grouped together in describing risk should be consistent and defined prior to ranking.

B.10.3.6 Reference documents

[89] ELMONSTRI, Mustafa, *Review of the strengths and weaknesses of risk matrices*

[90] BAYBUTT, Paul, *Calibration of risk matrices for process safety*

B.10.4 S-curves

B.10.4.1 Overview

Where a risk might have a range of consequence values, they can be displayed as a probability distribution of consequences (PDF). See, for example, the solid curve in Figure B.18. The data can also be plotted as a cumulative distribution (CDF), sometimes referred to as an S-curve (dashed line in Figure F.18). The PDF may be parametric or non-parametric.

The probability that a consequence will exceed a particular value can be directly read off the S-curve. For example, Figure B.18 indicates that there is a 90 % probability the consequences will not exceed consequence value C.

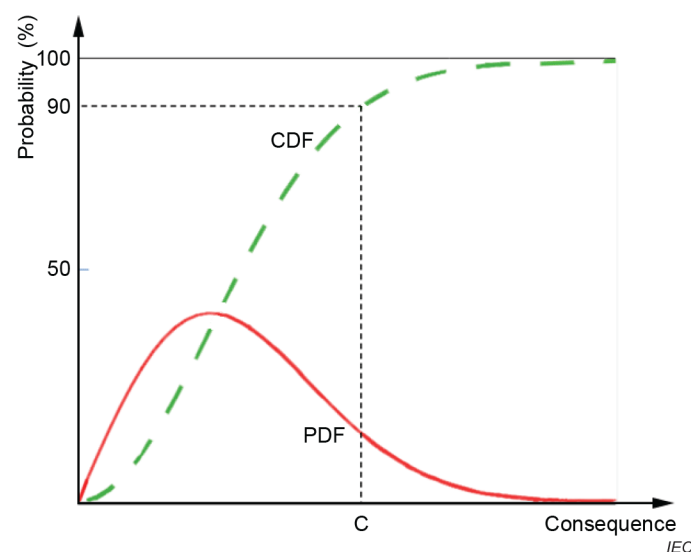


Figure B.18 – Probability distribution function and cumulative distribution function

In some cases the shape of the distribution is known on theoretical grounds. In others the shape of the distribution can be obtained from data or is the output of a model.

It is also possible to use expert judgment to estimate the low point of the consequence range, the likely mid-point, and the upper point of the range. Various formulae can then be used to determine the mean value for the consequence and the variance, and a curve can be plotted from this information.

B.10.4.2 Use

A pdf indicates the probability of different consequence values in a visual form that shows the most likely value, the extent of variability, and the extent to which there is a likelihood of an extreme event.

In some circumstances it can be useful to obtain a single representative value from the probability distribution, for example to compare with evaluation criteria. Often the expected value (equivalent to the mean) is used to represent the best estimate of the magnitude of consequences. (This is equivalent to the sum of the products of probabilities and consequence represented by the curve.) Other measures include the variance of the distribution or some percentile range such as the interquartile spread (the scale width enclosed by the 25th and the 75th percentile) or 5th and 95th percentile (see for example VaR B.7.2). However such measures might still not give sufficient emphasis to the possibility of extreme consequences, which can be important to the decisions to be made. For example, in selecting an investment, both the expected return and the fluctuations in returns are taken into account; in planning how to respond to fire, extreme events need to be considered as well as expected consequences.

The S-curve is a useful tool when discussing consequence values that represent an acceptable risk. It is a means of presenting data that makes it easier to see the probability that consequences will exceed a particular value.

B.10.4.3 Inputs

Producing an S-curve requires data or judgements from which a valid distribution can be produced. Although distributions can be produced by judgement with little data, the validity of the distribution and the statistics obtained from it will be greater the more data is available.

B.10.4.4 Outputs

The outputs are a diagram which can be used by decision makers when considering acceptability of a risk, and various statistics from the distribution that can be compared with criteria.

B.10.4.5 Strengths and limitations

Strengths include the following.

- The technique represents the magnitude of a risk where there is a distribution of consequences.
- Experts can usually make judgments of maximum, minimum and most likely values of consequence and produce a reasonable estimate of the likely shape of a distribution. Transferring this to the form of a cumulative distribution makes it easier for a lay person to use this information. As more and reliable input data are available, the accuracy of the S-curve improves.

Limitations include the following.

- The method can give an impression of accuracy which is not justified by the level of certainty of the data from which the distribution was produced.
- For any method of obtaining a point value or values to represent a distribution of consequences, there are underlying assumptions and uncertainties about:
 - the form of the distribution (e.g. normal, discrete, or highly skewed);
 - the most appropriate way of representing that distribution as a point value;
 - the value of the point estimate because of inherent uncertainties in the data from which it is derived.
- Distributions and their statistics based on experience or past data still provide little information on the likelihood of future events with extreme consequences but low likelihood.

B.10.4.6 Reference document

- [91] GARVEY, P., BOOK S.A., COVERT R.P. *Probability Methods for Cost Uncertainty Analysis: A Systems Engineering Perspective*

Bibliography

General

- [1] Principe "GAME" (*Globalement au moins équivalent*) *Methodologie de demonstration, Les guides d'application*. Systèmes de transport public guidés urbains de personnes. 2011
- [2] FEKETE ISTVAN, *Integrated Risk Assessment for supporting Management decisions* Scholars Press, Saarbrücken, Germany 2015
- [3] PEACE, C. The reasonably practicable test and work health and safety-related risk assessments *New Zealand Journal of Employment Relations*. 2017, 42(2), 61-78."

Techniques for eliciting views from stakeholders and experts

- [4] EN 12973, *Value Management*
- [5] PROCTOR, A. *Creative problem solving for managers*. Abingdon: Routledge
- [6] GOLDENBERG, Olga, WILEY, Jennifer. Quality, conformity, and conflict: Questioning the assumptions of Osborn's brainstorming technique, *The Journal of Problem Solving*. 2011, 3(2), 96-108 [viewed 2019-02-13] available at: <http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1093&context=jps>
- [7] ROWE, G. WRIGHT, G. The Delphi technique: Past, present, and future prospects. *Technological forecasting and social change*. 2011, 78, Special Delphi Issue
- [8] MCDONALD, D. BAMMER, G. and DEANE, P. *Research Integration Using Dialogue Methods*, ANU press Canberra. 2009 Chapter 3 Dialogue methods for understanding a problem: integrating judgements. Section 7 Nominal Group Technique [viewed 2019-02-13]. Available at <http://press.anu.edu.au/node/393/download>
- [9] HARRELL, M.C. BRADLEY, M.A. 2009 *Data collection methods – A training Manual – Semi structured interviews and focus groups*, RAND National defence research Institute USA [viewed 2019-02-13]. Available at: http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR718.pdf
- [10] GILL, J. JOHNSON, P. *Research methods for managers* 4th ed. 2010 London: Sage Publications Ltd
- [11] SAUNDERS, M. LEWIS, P. THORNHILL, A. *Research Methods for Business Students* 7th ed. 2016 Harlow: Pearson Education Ltd.
- [12] UNIVERSITY OF KANSAS COMMUNITY TOOL BOX Section 13 *Conducting surveys*; [viewed 2019-02-13]. Available at: <https://ctb.ku.edu/en/table-of-contents/assessment/assessing-community-needs-and-resources/conduct-surveys/main>

Techniques for identifying risk

- [13] MATHERLY, Carter *The Red Teaming Essential: Social Psychology Premier for Adversarial Based Alternative Analysis*. 2013 [viewed 2019-02-13]. Available at: <https://works.bepress.com/matherly/6/download/>

- [14] *Pestle analysis* Free Management eBooks [viewed 2019-02-13]. Available at: <http://www.free-management-ebooks.com/dldebk/dlst-pestle.htm>
- [15] POPOV, G., LYON, B., HOLLICROFT, B., *Risk Assessment: A Practical Guide to Assessing Operational Risks*. Hoboken, NJ: Wiley, 2016
- [16] IEC 62740, *Root cause analysis (RCA)*
- [17] BROUGHTON, Vanda. *Essential classification*. Facet Publishing 2015
- [18] BAILEY, Kenneth. Typologies and taxonomies: An introduction to classification technique. *Quantitative applications in the social sciences* Series 7,102 1994 Sage publications
- [19] VDI 2225 Blatt 1, *Konstruktionsmethodik- Technisch-wirtschaftliches Konstruieren - Vereinfachte Kostenermittlung*, 1997 Beuth Verlag
- [20] IEC 60812, *Failure modes and effects analysis (FMEA and FMECA)*
- [21] IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*
- [22] RINGLAND, Gill. *Scenarios in business*, Chichester: John Wiley, 2002
- [23] Van der HEIJDEN, Kees. *Scenarios: The art of strategic conversation*, Chichester; John Wiley, 2005
- [24] CHERMACK, Thomas J. *Scenario planning in organizations*, San Francisco: Berrett Koehler publishers Inc. 2011
- [25] MUKUL PAREEK, *Using Scenario analysis for managing technology risk*: [viewed 2019-02-13]. Available at: <http://www.isaca.org/Journal/archives/2012/Volume-6/Pages/Using-Scenario-Analysis-for-Managing-Technology-Risk.aspx>
- [26] CARD, Alan J. WARD, James R. and CLARKSON, P. John. Beyond FMEA: The structured what-if technique (SWIFT) *Journal of Healthcare Risk Management*, 2012, 31,(4) 23–29

Techniques for determining sources, causes and drivers of risk

- [27] KERVERN, G-Y. *Elements fondamentaux des cindyniques*, Editions Economica 1995
- [28] KERVERN, G-Y. *Latest advances in cindynics*, Editions Economica, 1994
- [29] KERVERN, G-Y. & BOULENGER, P. *Cindyniques – Concepts et mode d'emploi*, Edition Economica 2007
- [30] ISHIKAWA, K. *Guide to Quality Control*, Asia Productivity Organization, 1986

Techniques to analyse existing controls

- [31] LEWIS, S. SMITH, K., *Lessons learned from real world application of the bow-tie method. 6th AIChE. Global Congress of Process Safety*, 2010, San Antonio, Texas [viewed 2019-02-13]. Available at: <http://risktecsolutions.co.uk/media/43525/bow-tie%20lessons%20learned%20-%20aiche.pdf>

- [32] HALE, A. R., GOOSSENS L.H.J., ALE, B.J.M., BELLAMY L.A. POST J. *Managing safety barriers and controls at the workplace. In Probabilistic safety assessment and management.* Editors SPITZER C, SCHMOCKER, U, DANG VN,. Berlin: Springer; 2004. pp. 608–13
- [33] MCCONNELL, P. and DAVIES, M. *Scenario Analysis under Basel II.* [viewed 2019-02-13]. Available at <http://www.continuitycentral.com/feature0338.htm>
- [34] ISO 22000, *Food safety management systems – Requirements for any organization in the food chain*
- [35] *Food Quality and Safety Systems – A Training Manual on Food Hygiene and the Hazard Analysis and Critical Control Point (HACCP) System* [viewed 2019-02-13]. Available at <http://www.fao.org/docrep/W8088E/w8088e05.htm>
- [36] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*
- [37] IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*
- [38] CENTRE FOR CHEMICAL PROCESS SAFETY OF THE AMERICAN INSTITUTE OF CHEMICAL ENGINEERS New York 2001. *Layer of protection analysis – Simplified process risk assessment*

Techniques for understanding consequence and likelihood

- [39] GHOSH, J., DELAMPADY, M. and SAMANTA, T. *An introduction to Bayesian analysis, New York Springer-Verlag, 2006*
- [40] QUIGLEY, J.L., BEDFORD, T.J. and WALLS, L.A. Prior Distribution Elicitation. In: *Encyclopaedia of Statistics in Quality and Reliability.* Wiley. 2008 ISBN 9780470018613
- [41] NEIL, Martin and FENTON, Norman. *Risk Assessment and Decision Analysis with Bayesian Networks.* CRC Press, 2012
- [42] JENSEN, F.V., NIELSEN T. D. *Bayesian Networks and Decision Graphs*, 2nd ed. Springer, New York, 2007
- [43] NICHOLSON, A., WOODBERRY O and TWARDY C, *The "Native Fish" Bayesian networks.* Bayesian Intelligence Technical Report 2010/3, 2010
- [44] NETICA TUTORIAL Introduction to Bayes Nets: What is a Bayes Net? [viewed 2019-02-13]. Available at https://www.norsys.com/tutorials/netica/secA/tut_A1.htm
- [45] ISO/TS 22317, *Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA)*
- [46] ISO 22301, *Societal security – Business continuity management systems – Requirements*
- [47] ANDREWS J.D, RIDLEY L.M. 2002. Application of the cause-consequence diagram method to static systems, *Reliability engineering and system safety* 75(1) 47-58: also at <https://dspace.lboro.ac.uk/dspace-jspui/bitstream/2134/695/1/01-22.pdf> [viewed 2019-02-13]

- [48] NIELSEN D.S. The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis, Danish Atomic Energy Commission, RISO-M-1374, May 1971
- [49] IEC 62502, *Analysis techniques for dependability – Event tree analysis (ETA)*
- [50] IEC TR 63039:2016, *Probabilistic risk analysis of technological systems – Estimation of final event rate at a given initial state*
- [51] IEC 62508, *Guidance on human aspects of dependability*
- [52] BELL Julie, HOLROYD Justin, *Review of human reliability assessment methods*. Health and Safety Executive UK, HMSO 2009, [viewed 2019-02-13]. Available at <http://www.hse.gov.uk/research/rrpdf/rr679.pdf>
- [53] OECD Establishing the Appropriate Attributes in Current Human Reliability Assessment Techniques for Nuclear Safety, NEA/CSNI/R 2015 [viewed 2019-02-13] Available at: [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=NEA/CSNI/R\(2015\)1&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=NEA/CSNI/R(2015)1&docLanguage=En)
- [54] IEC 61165, *Application of Markov techniques*
- [55] OXLEY, ALAN. Markov Processes in Management Science, published by Applied Probability Trust, 2011 [viewed 2019-02-13]. Available at <https://studylib.net/doc/8176892/markov-processes-in-management-science>
- [56] ISO/IEC Guide 98-3:2008/Suppl.1:2008, *Uncertainty of measurement – Part 3: Guide to the expression of uncertainty in measurement (GUM:1995) – Supplement 1: Propagation of distributions using a Monte Carlo method*
- [57] EU: General Data Protection Regulation (European Union Official Journal, 04.05.2016)
- [58] ICO (UK): *Conducting privacy impact assessments code of practice* [viewed 2019-02-13] Available at: <https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf>
- [59] CNIL (FR), *Privacy Impact assessment (PIA)* [viewed 2019-02-13]. Available at: <https://www.cnil.fr/en/privacy-impact-assessment-pia>

Techniques for analysing dependencies and interactions

- [60] BRYSON, J. M., ACKERMANN, F., EDEN, C., & FINN, C. (2004). *Visible thinking unlocking causal mapping for practical business results*. Chichester: John Wiley & Sons
- [61] ACKERMANN, F, HOWICK, S, QUIGLEY, J, WALLS, L, HOUGHTON, T. Systemic risk elicitation: Using causal maps to engage stakeholders and build a comprehensive view of risks, *European Journal of Operational Research* 2014, 238(1), 290-299
- [62] JOINT RESEARCH CENTRE, EUROPEAN COMMISSION, *Cross-impact analysis* [viewed 2019-02-13] Available at: http://forlearn.jrc.ec.europa.eu/guide/2_design/meth_cross-impact-analysis.htm

Techniques to provide a measure of risk

- [63] WORLD HEALTH ORGANISATION Human health risk assessment toolkit – chemical hazards. 2010 [viewed 2019-02-13]. Available at <http://www.inchem.org/documents/harmproj/harmproj/harmproj8.pdf>
- [64] US EPA *Guidelines for ecological risk assessment* 1998 [viewed 2019-02-13]. Available at https://www.epa.gov/sites/production/files/2014-11/documents/eco_risk_assessment1998.pdf
- [65] CHANCE, D., BROOKS, R. *An introduction to derivatives and risk management*, (9th ed.). Published Mason, Ohio: South-Western Cengage Learning 2013
- [66] THOMAS J. and PEARSON Neil D. Value at risk. *Financial Analysts Journal* 2000 56, 47-67
- [67] CHOUDHRY , M. *An introduction to Value at Risk*, Ed. 5, John Wiley and Sons, Chichester UK, 2013
- [68] *Value at Risk* New York University. [viewed 2019-02-13]. Available at: <http://people.stern.nyu.edu/adamodar/pdfiles/papers/VAR.pdf>

Techniques for evaluating the significance of risk

- [69] UK HEALTH AND SAFTY EXECUTIVE, 2010a: *HID'S Approach To 'As Low As Reasonably Practicable' (ALARP) Decisions* [viewed 2019-02-13] available at: <http://www.hse.gov.uk/risk/theory/alarpglance.htm>
- [70] UK HEALTH AND SAFTY EXECUTIVE, 2010b: *Guidance on (ALARP) decisions in control of major accident hazards (COMAH)*, [viewed 2019-02-13] available at: http://www.hse.gov.uk/foi/internalops/hid_circs/permissioning/spc_perm_37/
- [71] UK HEALTH AND SAFTY EXECUTIVE, 2014: *Principles and guidelines to assist HSE in its judgments that duty-holders have reduced risk as low as reasonably practicable* [viewed 2019-02-13] available at: <http://www.hse.gov.uk/risk/theory/alarp1.htm>
- [72] AMERICAN INSTITUTE FOR CHEMICAL ENGINEERS: *Understanding and using F-N Diagrams: Annex A in Guidelines for Developing Quantitative Safety Risk Criteria*. New York. John Wiley 2009
- [73] EVANS, A. *Transport fatal accidents and FN-curves: 1967-2001*. Health and Safety Executive Research Report RR 073 [viewed 2019-02-13]. Available at: <http://webarchive.nationalarchives.gov.uk/20101111125221/http://www.rail-reg.gov.uk/upload/pdf/rr073.pdf>
- [74] *Pareto Chart, Excel Easy* [viewed 2019-02-13]. Available at: <http://www.excel-easy.com/examples/pareto-chart.html>
- [75] *Pareto Chart* [viewed 2019-02-13]. Available at: <http://www.uphs.upenn.edu/gme/pdfs/Pareto%20Chart.pdf>
- [76] IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*
- [77] MACKENZIE Cameron A. *Summarizing risk using risk measures and risk indices*. *Risk Analysis*, 34,12 2143-2163 2014

Techniques for selecting between options

- [78] KHOJASTEH, P, (2016). Application of benefit-cost-risk formula and key change indicators to meet project objectives [viewed 2019-02-13]. Available at <https://www1.bournemouth.ac.uk/sites/default/files/asset/document/Mon%205.1%20Khojasteh%20Pejman%20Risk.pdf>
- [79] The Green book, Appraisal and Evaluation in Central Government; 2011 Treasury Guidance LONDON: TSO London
- [80] ANDOSEH, S., et al. The case for a real options approach to ex-ante cost-benefit analyses of agricultural research projects. *Food policy* 44, 2014, 218-226 [viewed 2019-02-13]. Available at: http://pdf.usaid.gov/pdf_docs/pnaec758.pdf
- [81] KIRKWOOD, CRAIG . Decision Tree Primer University of Arizona in *Decision Analysis and System Dynamics resources* 2002 [viewed 2019-02-13]. Available at: <http://www.public.asu.edu/~kirkwood/DASstuff/decisiontrees/>
- [82] MYERSON, ROGER B., *Game Theory: Analysis of Conflict*, Harvard University Press, 1991
- [83] MARYNARD, SMITH JOHN *Evolution and Theory of Games*, Cambridge University Press 1982
- [84] ROSENHEAD, J. and MINGER, J. (Eds), *Rational Analysis for a Problematic World Revisited*, 2nd ed. Wiley, Chichester UK, 2001
- [85] EN 16271:2012, *Value management – Functional expression of the need and functional performance specification – Requirements for expressing and validating the need to be satisfied within the process of purchasing or obtaining a product*
- [86] DEPARTMENT FOR COMMUNITIES AND LOCAL GOVERNMENT, *Multi-criteria analysis: a manual* 2009 [viewed 2019-02-13]. Available at: <https://www.gov.uk/government/publications/multi-criteria-analysis-manual-for-making-government-policy>
- [87] RABIHAH MHD.SUM, *Risk Management Decision Making*, 2001 [viewed 2019-02-13]. Available at: <http://www.isahp.org/uploads/47.pdf>
- [88] VELASQUEZ, M., HESTER, P. An Analysis of Multi-criteria Decision Making Methods, *International Journal of Operations Research*, 10 (2), 55-66, 2013 [viewed 2019-02-13]. Available at: http://www.orstw.org.tw/ijor/vol10no2/ijor_vol10_no2_p56_p66.pdf

Techniques for recording and reporting

- [89] ELMONSTRI, Mustafa, *Review of the strengths and weaknesses of risk matrices*, *Journal of Risk Analysis and Crisis Response*, 4 (1), 49-57, 2014 [viewed 2019-02-13]. Available at http://www.atlantis-press.com/php/download_paper.php?id=11718
- [90] BAYBUTT, Paul, Calibration of risk matrices for process safety. *Journal of Loss Prevention in the Process Industries*, 38, 163-168, 2015
- [91] GARVEY, P., BOOK S.A., COVERT R.P. *Probability Methods for Cost Uncertainty Analysis: A Systems Engineering Perspective*, Ed 2 Annex E Unravelling the S curve. CRC 2016

SOMMAIRE

AVANT-PROPOS	130
INTRODUCTION.....	132
1 Domaine d'application	133
2 Références normatives	133
3 Termes et définitions	133
4 Concepts centraux.....	134
4.1 Incertitude.....	134
4.2 Risque	135
5 Utilisations des techniques d'appréciation du risque	135
6 Mise en œuvre de l'appréciation du risque.....	137
6.1 Planification de l'appréciation.....	137
6.1.1 Définition de l'objet et du domaine d'application de l'appréciation	137
6.1.2 Compréhension du contexte	137
6.1.3 Collaboration avec les parties prenantes	137
6.1.4 Définition des objectifs	138
6.1.5 Prise en compte des facteurs humains, organisationnels et sociaux	138
6.1.6 Revue des critères de décision	139
6.2 Gestion des informations et développement de modèles	140
6.2.1 Généralités	140
6.2.2 Collecte d'informations	141
6.2.3 Analyse des données.....	141
6.2.4 Développement et application des modèles	142
6.3 Application des techniques d'appréciation du risque	143
6.3.1 Vue d'ensemble	143
6.3.2 Identification du risque	144
6.3.3 Détermination des sources, des causes et des facteurs de risque	145
6.3.4 Examen de l'efficacité des moyens de maîtrise existants	145
6.3.5 Compréhension des conséquences et de la vraisemblance.....	146
6.3.6 Analyse des interactions et des dépendances.....	148
6.3.7 Compréhension des mesures du risque	148
6.4 Examen de l'analyse	151
6.4.1 Vérification et validation des résultats.....	151
6.4.2 Analyse d'incertitude et de sensibilité	151
6.4.3 Surveillance et revue	152
6.5 Application des résultats à l'appui des décisions	152
6.5.1 Vue d'ensemble	152
6.5.2 Décisions relatives à l'importance du risque	153
6.5.3 Décisions impliquant de choisir parmi des options	153
6.6 Enregistrement et consignation du processus d'appréciation du risque et de ses résultats	154
7 Choix des techniques d'appréciation du risque	155
7.1 Généralités	155
7.2 Choix des techniques.....	155
Annexe A (informative) Catégorisation des techniques.....	157
A.1 Introduction à la catégorisation des techniques.....	157
A.2 Application de la catégorisation des techniques	157

A.3	Utilisation des techniques au cours du processus ISO 31000	165
Annexe B (informative) Description des techniques.....		168
B.1	Techniques permettant de faire émerger les points de vue des parties prenantes et des experts.....	168
B.1.1	Généralités	168
B.1.2	"Brainstorming".....	169
B.1.3	Technique Delphi.....	170
B.1.4	Technique des groupes nominaux.....	171
B.1.5	Entretiens structurés ou semi-structurés	173
B.1.6	Enquêtes	174
B.2	Techniques d'identification du risque	175
B.2.1	Généralités	175
B.2.2	Listes de contrôle, classifications et taxonomies	176
B.2.3	Analyse des modes de défaillance et de leurs effets (AMDE) et analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC).....	178
B.2.4	Etudes de danger et d'exploitabilité (HAZOP)	180
B.2.5	Analyse du scénario	182
B.2.6	Méthode SWIFT ("Que se passerait-il si?")	184
B.3	Techniques de détermination des sources, causes et facteurs de risque.....	186
B.3.1	Généralités	186
B.3.2	Approche cindynique	186
B.3.3	Méthode d'Ishikawa (diagramme en arêtes de poisson)	188
B.4	Techniques d'analyse des moyens de maîtrise.....	190
B.4.1	Généralités	190
B.4.2	Analyse "nœud papillon"	191
B.4.3	Analyse des dangers – points critiques pour leur maîtrise (HACCP)	193
B.4.4	Méthode LOPA	195
B.5	Techniques permettant de comprendre les conséquences et la vraisemblance.....	197
B.5.1	Généralités	197
B.5.2	Analyse bayésienne.....	198
B.5.3	Réseaux bayésiens et diagrammes d'influence	200
B.5.4	Analyse d'impact sur l'activité (AIA)	202
B.5.5	Analyse causes-conséquences (ACC)	204
B.5.6	Analyse par arbre d'événement (AAE)	206
B.5.7	Analyse par arbre de panne (AAP).....	208
B.5.8	Analyse de fiabilité humaine (AFH)	210
B.5.9	Analyse de Markov	212
B.5.10	Simulation de Monte-Carlo	214
B.5.11	Analyse d'impact sur la vie privée (PIA) / analyse d'impact sur la protection des données (DPIA)	217
B.6	Techniques d'analyse des dépendances et des interactions.....	219
B.6.1	Cartographie causale.....	219
B.6.2	Analyse d'impacts croisés.....	221
B.7	Techniques utilisées pour produire une mesure du risque	223
B.7.1	Appréciation du risque toxicologique.....	223
B.7.2	Valeur en risque (VaR)	225
B.7.3	Valeur en risque conditionnelle (CVaR) ou "expected shortfall" (ES).....	227
B.8	Techniques d'évaluation de l'importance d'un risque	228
B.8.1	Généralités	228

B.8.2	Critères ALARP et SFAIRP	229
B.8.3	Diagrammes fréquence-nombre (F-N).....	231
B.8.4	Diagrammes de Pareto	233
B.8.5	Maintenance basée sur la fiabilité (MBF)	235
B.8.6	Indices de risque	238
B.9	Techniques de choix parmi des options.....	240
B.9.1	Généralités	240
B.9.2	Analyse coût/bénéfice (ACB)	240
B.9.3	Analyse par arbre de décision.....	242
B.9.4	Théorie des jeux	244
B.9.5	Analyse à critères multiples (ACM)	246
B.10	Techniques d'enregistrement et de consignation	248
B.10.1	Généralités	248
B.10.2	Registres des risques	249
B.10.3	Matrice conséquence/vraisemblance (matrice de risque ou carte thermique)	251
B.10.4	Courbes en S	255
Bibliographie.....		258
Figure A.1 – Application des techniques au processus de management du risque ISO 31000 [3]		165
Figure B.1 – Exemple de diagramme d'Ishikawa (en arêtes de poisson).....		189
Figure B.2 – Exemple de "nœud papillon"		191
Figure B.3 – Réseau bayésien montrant une version simplifiée d'un problème écologique réel: modélisation des populations de poissons autochtones dans l'Etat de Victoria en Australie.....		200
Figure B.4 – Exemple de diagramme causes-conséquences		205
Figure B.5 – Exemple d'analyse par arbre d'événement		207
Figure B.6 – Exemple d'arbre de panne		209
Figure B.7 – Exemple de diagramme de Markov		213
Figure B.8 – Exemple de courbe dose-effet		223
Figure B.9 – Distribution de la valeur		226
Figure B.10 – Détail des valeurs de la VaR dans la zone de pertes.....		226
Figure B.11 – VaR et CVaR pour un portefeuille présentant une perte possible		228
Figure B.12 – Diagramme ALARP		230
Figure B.13 – Exemple de diagramme F-N.....		232
Figure B.14 – Exemple de diagramme de Pareto		234
Figure B.15 – Exemple partiel de tableau définissant les échelles de conséquences.....		251
Figure B.16 – Exemple partiel d'échelle de vraisemblance		252
Figure B.17 – Exemple de matrice conséquence-vraisemblance		253
Figure B.18 – Fonction de distribution de la probabilité et fonction de distribution cumulative		255
Tableau A.1 – Caractéristiques des techniques.....		157
Tableau A.2 – Techniques et caractéristiques indicatives		158
Tableau A.3 – Applicabilité des techniques au processus ISO 31000		166

Tableau B.1 – Exemple de mots-guides fondamentaux et de leurs significations génériques.....	181
Tableau B.2 – Tableau des déficits pour chaque partie prenante	187
Tableau B.3 – Tableau des dissonances entre les parties prenantes	188
Tableau B.4 – Exemple de matrice de Markov	213
Tableau B.5 – Exemples de systèmes auxquels l'analyse de Markov peut s'appliquer.....	214
Tableau B.6 – Exemple de choix des tâches avec la MBF	237
Tableau B.7 – Exemple de matrice de jeu	245

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

MANAGEMENT DU RISQUE – TECHNIQUES D'APPRÉCIATION DU RISQUE

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 31010 a été établie par le comité d'études 56 de l'IEC: Sûreté de fonctionnement, en coopération avec le comité d'études 262 de l'ISO: Management du risque.

Elle est publiée en tant que norme double logo.

Cette deuxième édition annule et remplace la première édition parue en 2009. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- les processus de planification, de mise en œuvre, de vérification et de validation de l'utilisation des techniques sont décrits de manière plus précise;
- le nombre et la plage d'application des techniques ont été élargis;

- les concepts couverts par l'ISO 31000 ne sont plus traités dans la présente norme.

Le texte de la présente Norme internationale est issu des documents suivants de l'IEC:

FDIS	Rapport de vote
56/1837/FDIS	56/1845/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette Norme internationale. A l'ISO, la norme a été approuvée par 44 membres P sur un total de 46 votes exprimés.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "*colour inside*" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Le présent document donne des recommandations pour le choix et l'application des différentes techniques pouvant être utilisées afin d'améliorer la prise en considération de l'incertitude et le management du risque.

Les techniques sont utilisées:

- lorsqu'il est nécessaire d'effectuer une analyse approfondie pour identifier les risques existants ou un risque particulier;
- dans le cadre d'une décision où différentes options, chacune impliquant des risques, nécessitent d'être comparées ou optimisées;
- dans le cadre d'un processus de management du risque donnant lieu à des actions de traitement du risque.

Les techniques sont utilisées au cours de la procédure d'appréciation du risque visant à identifier, analyser et évaluer le risque (décrite dans l'ISO 31000) et, de manière plus générale, à chaque fois qu'il s'avère nécessaire d'appréhender l'incertitude et ses effets.

Les techniques décrites dans le présent document peuvent être utilisées dans différents contextes, mais plus largement dans le domaine technique. Certaines techniques sont similaires d'un point de vue conceptuel, mais leurs différents noms et méthodologies reflètent l'historique de leur développement dans différents secteurs. Les techniques ont évolué dans le temps et continuent d'évoluer. La plupart d'entre elles peuvent être utilisées dans de nombreuses situations, hors de leur application d'origine. Les techniques peuvent être adaptées, combinées et appliquées sous de nouvelles formes ou étendues afin de répondre aux besoins présents ou futurs.

Le présent document est une introduction aux techniques choisies. Elle compare leurs applications possibles, leurs avantages et leurs limites. Elle fait également référence à des sources d'informations plus précises.

Le présent document s'adresse éventuellement:

- à quiconque est concerné par l'appréciation ou le management du risque;
- aux personnes qui établissent les recommandations visant à établir la manière dont le risque doit être apprécié dans des contextes particuliers;
- aux personnes qui ont besoin de prendre des décisions en cas d'incertitude, notamment:
 - les personnes qui mettent en œuvre ou procèdent à des appréciations du risque;
 - les personnes qui ont besoin de comprendre les résultats des appréciations;
 - les personnes qui doivent choisir des techniques d'appréciation pour répondre à des besoins particuliers.

Les organisations qui sont tenues de procéder à des appréciations du risque pour les besoins de la conformité gagneraient à utiliser des techniques d'appréciation du risque formelles et normalisées appropriées.

MANAGEMENT DU RISQUE – TECHNIQUES D'APPRÉCIATION DU RISQUE

1 Domaine d'application

La présente Norme internationale donne des recommandations pour le choix et l'application des techniques d'appréciation du risque dans différentes situations. Ces techniques visent à aider à la prise de décision en cas d'incertitude, à donner des informations relatives à des risques particuliers et dans le cadre d'un processus de management du risque. Le document récapitule l'éventail des techniques, avec des références vers d'autres documents où ces techniques sont décrites de manière plus précise.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

Guide ISO 73:2009, *Management du risque – Vocabulaire*

ISO 31000:2018, *Management du risque – Lignes directrices*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO 31000:2018 et du Guide ISO 73:2009 ainsi que les suivants, s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse <http://www.electropedia.org/>
- ISO Online browsing platform: disponible à l'adresse <http://www.iso.org/obp>

3.1

vraisemblance

possibilité que quelque chose se produise

Note 1 à l'article: Dans la terminologie du management du risque, le terme "vraisemblance" est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques (telles une probabilité ou une fréquence sur une période donnée).

Note 2 à l'article: Le terme anglais "*likelihood*" (vraisemblance) n'a pas d'équivalent direct dans certaines langues et c'est souvent l'équivalent du terme "*probability*" (probabilité) qui est utilisé à la place. En anglais, cependant, le terme "*probability*" (probabilité) est souvent limité à son interprétation mathématique. Par conséquent, dans la terminologie du management du risque, le terme «vraisemblance» est utilisé avec l'intention qu'il fasse l'objet d'une interprétation aussi large que celle dont bénéficie le terme "*probability*" (probabilité) dans de nombreuses langues autres que l'anglais.

[SOURCE: ISO 31000:2018, 3.7]

3.2

opportunité

combinaison de circonstances attendues comme favorables aux objectifs

Note 1 à l'article: Une opportunité est une situation positive susceptible de produire un gain et sur laquelle on dispose d'un certain niveau de contrôle.

Note 2 à l'article: Une opportunité pour une partie peut constituer une menace pour une autre partie.

Note 3 à l'article: La saisie ou la non-saisie d'une opportunité constitue l'une comme l'autre une source de risque.

3.3

probabilité

mesure des chances d'occurrence, exprimée par un nombre compris entre 0 et 1, où 0 désigne une impossibilité et 1 une certitude absolue

Note 1 à l'article: Voir définition 3.1, Note 2 à l'article.

3.4

facteur de risque

facteur ayant une influence importante sur le risque

3.5

menace

source potentielle de danger, de nuisance ou d'un autre résultat indésirable

Note 1 à l'article: Une menace est une situation négative susceptible d'entraîner une perte et sur laquelle on dispose de relativement peu de contrôle.

Note 2 à l'article: Une menace pour une partie peut constituer une opportunité pour une autre partie.

4 Concepts centraux

4.1 Incertitude

Le terme "incertitude" englobe de nombreux concepts sous-jacents. Les types d'incertitudes ont fait, et continuent de faire, l'objet de nombreuses tentatives de catégorisation, notamment:

- l'incertitude qui reconnaît la variabilité intrinsèque de certains phénomènes et qui ne peut pas être réduite par une recherche approfondie (parfois appelée incertitude aléatoire), comme un jet de dés, par exemple;
- l'incertitude qui, en règle générale, est le fruit d'un manque de connaissances et qui peut donc être réduite en collectant plus de données, en affinant des modèles, en améliorant les techniques d'échantillonnage (parfois appelée incertitude épistémique).

Les incertitudes suivantes sont d'autres formes d'incertitude couramment admises:

- l'incertitude linguistique, qui reconnaît le caractère vague et ambigu inhérent aux langues parlées;
- l'incertitude de décision, qui revêt une importance particulière pour les stratégies de management du risque, et qui identifie l'incertitude liée aux systèmes de valeur, au jugement professionnel, aux valeurs d'entreprise et aux normes sociétales.

Exemples d'incertitudes:

- l'incertitude relative aux interprétations, y compris les hypothèses quant à la manière dont les personnes se comportent;
- la variabilité des paramètres sur lesquels doit reposer une décision;
- l'incertitude quant à la validité ou l'exactitude des modèles qui ont été établis pour faire des prévisions sur l'avenir;
- les événements (y compris les changements de circonstances ou de conditions) dont l'occurrence, le caractère ou les conséquences sont incertains;
- l'incertitude liée aux sinistres;

- l'issue incertaine des problèmes systémiques, comme les pénuries de personnel compétent, pouvant avoir des impacts considérables qui ne peuvent pas être clairement définis;
- le manque de connaissances qui apparaît lorsque l'incertitude est reconnue, mais pas totalement comprise;
- l'imprévisibilité;
- l'incertitude liée aux limites de l'esprit humain, par exemple dans la compréhension de données complexes, la prévision de situations ayant des conséquences à long terme ou la formulation de jugements impartiaux.

Toutes les incertitudes ne sont pas propres à être comprises. En outre, l'importance d'une incertitude peut être difficile, voire impossible, à définir ou influencer. Toutefois, la reconnaissance de l'existence d'une incertitude dans un contexte spécifique permet de mettre en place très tôt des systèmes de mise en garde afin de détecter des changements de manière proactive et opportune et prendre des dispositions pour favoriser la résilience afin de mieux faire face aux situations imprévues.

4.2 Risque

Le risque inclut les effets de toutes les formes d'incertitude décrites en 4.1 sur les objectifs. L'incertitude peut avoir des conséquences positives et/ou négatives.

Le risque est souvent décrit en termes de sources de risques, d'événements potentiels, de leurs conséquences et de leurs vraisemblances. Un événement peut avoir plusieurs causes et conduire à de multiples conséquences. Les conséquences peuvent avoir un certain nombre de valeurs discrètes, être des variables continues ou être inconnues. Les conséquences peuvent ne pas être discernables ou mesurables à première vue, mais peuvent s'accumuler au fil du temps. Les sources de risques peuvent inclure la variabilité inhérente ou les incertitudes relatives à divers facteurs, notamment le comportement humain et les structures organisationnelles ou les influences sociétales, pour lesquels il peut être difficile de prévoir si un événement particulier est susceptible de se produire. Il s'ensuit que le risque ne peut pas toujours être aisément présenté sous la forme d'un ensemble d'événements, de leurs conséquences et de leurs vraisemblances.

Les techniques d'appréciation du risque visent à aider les personnes à appréhender l'incertitude et le risque associé dans ce contexte vaste, complexe et diversifié, avec pour objectif de venir à l'appui de décisions et d'actions mieux argumentées.

5 Utilisations des techniques d'appréciation du risque

Les techniques décrites dans le présent document offrent un moyen de mieux comprendre l'incertitude et ses implications dans les décisions et actions.

L'ISO 31000 décrit les principes de management du risque, ainsi que les processus et cadres organisationnels en rapport avec ce domaine. Elle spécifie un processus de reconnaissance, de compréhension et, le cas échéant, de modification du risque en fonction de critères établis dans le cadre de ce processus. Les techniques d'appréciation du risque peuvent être appliquées dans le cadre de cette approche structurée qui implique l'établissement d'un contexte, l'appréciation et le traitement du risque, avec une surveillance, une revue, une communication, une concertation, une consignation et un enregistrement en continu. Ce processus est représenté à la Figure A.1, qui donne également des exemples d'endroits où ces techniques peuvent être appliquées.

Dans le processus ISO 31000, l'appréciation du risque implique d'identifier les risques, de les analyser et de s'appuyer sur la compréhension acquise dans le cadre de l'analyse pour évaluer le risque en tirant des conclusions sur son importance comparative en fonction des objectifs et des seuils de performances de l'organisation. Ce processus contribue à la prise de décisions quant à savoir si un traitement est exigé, quant aux priorités en matière de

traitement et quant aux actions destinées à traiter le risque. Dans la pratique, une approche itérative est appliquée.

Les techniques d'appréciation du risque décrites dans le présent document sont utilisées:

- lorsqu'il est exigé de mieux comprendre les risques en présence ou un risque particulier;
- dans le cadre d'un processus de management du risque donnant lieu à des actions de traitement du risque;
- dans le cadre d'une décision où différentes options, chacune impliquant des risques, nécessitent d'être comparées ou optimisées.

En particulier, les techniques peuvent être utilisées pour:

- fournir des informations structurées venant à l'appui des décisions et des actions en cas d'incertitude;
- apporter des éclaircissements quant aux conséquences des hypothèses formulées sur l'atteinte des objectifs;
- comparer plusieurs options, systèmes, technologies ou approches, etc. lorsque chaque option fait l'objet d'une incertitude aux multiples facettes;
- faciliter la définition d'objectifs stratégiques et opérationnels réalistes;
- contribuer à déterminer les critères de risque d'une organisation (limites de risque, goût du risque ou capacité de prise de risque, par exemple);
- tenir compte du risque lors de la définition ou de la révision des priorités;
- reconnaître et comprendre le risque, y compris celui qui pourrait avoir des conséquences extrêmes;
- comprendre les incertitudes essentielles pour les objectifs d'une organisation et justifier ce qu'il convient de faire les concernant;
- reconnaître et exploiter les opportunités avec plus de succès;
- articuler clairement les facteurs qui contribuent au risque et les raisons pour lesquelles ils sont importants;
- identifier des traitements du risque efficaces et efficients;
- déterminer les effets modificateurs des traitements suggérés du risque, y compris toutes les modifications de la nature ou de l'ampleur du risque;
- communiquer à propos du risque et de ses implications;
- apprendre des réussites et des échecs pour améliorer la manière de gérer le risque;
- démontrer que les exigences réglementaires et autres ont été respectées.

La manière d'apprécier le risque dépend de la complexité et de la nouveauté de la situation, ainsi que du niveau de connaissance et de compréhension correspondant.

- Dans le cas le plus simple, si une situation ne présente rien de nouveau ou d'inhabituel, que le risque est bien compris, qu'aucune partie prenante n'est intervenue ou que les conséquences ne sont pas significatives, des actions sont susceptibles d'être décidées en fonction de règles et procédures établies et des précédentes appréciations du risque.
- Pour les questions sans précédent, complexes ou difficiles, si l'incertitude est élevée et l'expérience limitée, la quantité d'informations servant de base à l'appréciation est insuffisante et les techniques d'analyse conventionnelles peuvent ne pas être utiles ou pertinentes. Cela s'applique également aux situations, où les parties prenantes partagent des points de vue diamétralement opposés. Dans ces cas, plusieurs techniques peuvent être utilisées pour obtenir une compréhension partielle du risque, en formulant dans ce cas des jugements dans le contexte de valeurs organisationnelles et sociétales, et en tenant compte des points de vue des parties prenantes.

Les techniques décrites dans le présent document sont optimales entre ces deux situations extrêmes, dont la complexité est modérée et qui donnent des informations sur lesquelles repose l'appréciation.

6 Mise en œuvre de l'appréciation du risque

6.1 Planification de l'appréciation

6.1.1 Définition de l'objet et du domaine d'application de l'appréciation

Il convient de définir l'objet de l'appréciation, et en particulier d'identifier les décisions ou actions auxquelles il est lié, les décideurs, les parties prenantes, la périodicité et la nature du résultat exigé (si des informations qualitatives, semi-quantitatives ou quantitatives sont exigées, par exemple).

Il convient de définir le domaine d'application, l'étendue et le niveau de détail de l'appréciation, avec une description de ce qu'il contient et de ce qui en est exclu. Il convient de définir les types de conséquences à inclure dans l'appréciation. Il convient également de spécifier toutes les conditions, hypothèses, contraintes ou ressources nécessaires pertinentes pour l'appréciation.

6.1.2 Compréhension du contexte

Lors d'une appréciation du risque, il convient que les personnes impliquées aient conscience des circonstances plus générales dans lesquelles les décisions et actions reposant sur leur appréciation sont prises. Cela inclut une compréhension des questions internes et externes qui participent au contexte de l'organisation, ainsi que des aspects sociétaux et environnementaux plus généraux. Il convient de revoir et de vérifier toutes les déclarations de contexte pertinentes, de manière à savoir si elles sont à jour et appropriées. Il est particulièrement important d'avoir une vision globale en cas de complexité importante.

6.1.3 Collaboration avec les parties prenantes

Il convient d'identifier les parties prenantes et les personnes susceptibles d'être en mesure d'apporter des connaissances utiles ou des avis pertinents, et de tenir compte de leurs points de vue, qu'elles participent ou non à l'appréciation. La participation appropriée des parties prenantes permet de s'assurer que les informations sur lesquelles repose l'appréciation du risque sont valables et applicables, et que les parties prenantes ont bien compris les raisons qui motivent ces décisions. La participation des parties prenantes peut:

- donner des informations permettant de comprendre le contexte de l'appréciation;
- rassembler différents domaines de connaissance et d'expertise pour une meilleure identification et compréhension des risques;
- apporter l'expertise attendue pour l'utilisation des techniques;
- permettre de comprendre et de tenir compte des intérêts des parties prenantes;
- contribuer au processus de détermination du caractère acceptable du risque, en particulier si les parties prenantes sont touchées;
- satisfaire aux exigences des personnes à informer et consulter;
- obtenir un soutien pour les résultats obtenus et les décisions prises à la suite de l'appréciation du risque;
- identifier les manques de connaissances qu'il est nécessaire de résoudre avant et/ou pendant l'appréciation du risque.

Il convient de décider des moyens par lesquels les produits et les résultats de l'appréciation du risque doivent être communiqués de manière fiable, précise et transparente aux parties prenantes.

Les techniques permettant d'obtenir les points de vue des parties prenantes et des experts sont décrites à l'Article B.1.

6.1.4 Définition des objectifs

Il convient de définir et, dans la mesure du possible, de documenter les objectifs du système ou processus spécifique pour lequel est effectuée l'appréciation du risque. Ceci facilitera l'identification des risques et la compréhension de leurs implications.

Dans la mesure du possible, il convient que les objectifs soient:

- spécifiques à l'objet de l'appréciation;
- mesurables de manière qualitative ou quantitative;
- réalisables dans la limite des contraintes imposées par le contexte;
- pertinents du point de vue des objectifs plus généraux ou du contexte de l'organisation;
- réalisés dans un délai défini.

6.1.5 Prise en compte des facteurs humains, organisationnels et sociaux

Il convient de considérer les facteurs humains, organisationnels et sociaux de manière explicite et de les prendre en compte selon le cas. Les aspects humains sont pertinents pour l'appréciation du risque de la manière suivante:

- comme source d'incertitude;
- par leurs influences sur la manière de choisir et d'appliquer les techniques;
- dans la manière d'interpréter et d'utiliser les informations (en raison, par exemple, des différentes perceptions du risque).

Les performances humaines (au-delà ou en deçà des attentes) sont une source de risque et peuvent également avoir un impact sur l'efficacité des moyens de maîtrise. Il convient de prendre en compte l'éventualité d'une divergence par rapport aux comportements prévus ou supposés lors de l'appréciation du risque. Les considérations en matière de performances humaines sont souvent complexes, et une expertise peut être exigée pour identifier et analyser les aspects humains des risques.

Les facteurs humains ont également un impact sur le choix et l'utilisation des techniques, en particulier lorsque des jugements doivent être portés ou des approches collectives utilisées. Un animateur qualifié est nécessaire pour réduire le plus possible ces impacts. Il convient de tenir compte des partis pris (comme la pensée de groupe) et de l'excès de confiance (dans les estimations et les perceptions, par exemple). Dans toute la mesure du possible, il convient d'argumenter l'avis de l'expert au moyen de preuves et données, et de consentir des efforts pour éliminer ou réduire le plus possible les partis pris cognitifs.

Les objectifs et valeurs personnels peuvent varier et être différents de ceux de l'organisation. Cela peut donner lieu à des perceptions différentes du niveau d'un risque et à des critères de prise de décision différents en fonction des individus. Il convient qu'une organisation s'efforce d'obtenir une compréhension commune du risque en interne et tienne compte des différentes perceptions des parties prenantes.

Les aspects sociaux, notamment la situation socioéconomique, l'origine ethnique et la culture, le sexe, les relations sociales, le contexte résidentiel et communautaire peuvent avoir un impact tant direct qu'indirect sur le risque. Les impacts peuvent être à long terme et ne pas être visibles immédiatement, et peuvent exiger une perspective de planification à long terme.

6.1.6 Revue des critères de décision

6.1.6.1 Généralités

Il convient de revoir les critères, y compris les critères de risque, qu'il est nécessaire de prendre en compte lors de la prise de décision, avant de procéder à l'appréciation. Ces critères peuvent être qualitatifs, semi-quantitatifs ou quantitatifs. Dans certains cas, il peut ne pas y avoir de critères explicites spécifiés, et les parties prenantes s'appuient sur leur jugement pour répondre aux résultats de l'analyse.

Les critères pertinents à revoir sont les suivants:

- la manière de décider si le risque est acceptable;
- la manière dont est déterminée l'importance relative des risques;
- la manière dont le risque est pris en considération pour choisir parmi des options lorsque chacune d'elles est associée à plusieurs risques qui peuvent avoir des conséquences positives et/ou négatives;
- la manière dont seront prises en compte les relations entre les risques.

6.1.6.2 Critères pour décider si un risque peut être accepté

Les critères de définition de la nature et de l'étendue du risque qui peut être accepté pour atteindre des objectifs, parfois appelés "goût du risque", peuvent être définis en spécifiant une technique permettant de déterminer l'ampleur du risque, ou d'un paramètre lié au risque, en fixant une limite au-delà de laquelle le risque devient inacceptable. La limite fixée pour qu'un risque devienne inacceptable peut dépendre des éventuelles retombées.

L'acceptabilité du risque peut également être définie en spécifiant la variation acceptable des mesures de performances spécifiques liées aux objectifs.

Différents critères peuvent être spécifiés selon le type de conséquences. Par exemple, les critères d'une organisation pour accepter un risque financier peuvent être différents de ceux définis pour les risques pour la vie humaine.

Certains exemples de considérations utilisées pour définir si un risque peut être accepté sont présentés ci-dessous.

- Capacité de prise de risque (RBC – *risk bearing capacity*) (également appelée capacité de risque): la RBC d'une organisation est souvent définie par le capital de risque disponible pour absorber les effets néfastes des risques. Pour une entreprise commerciale, la capacité peut être spécifiée par la capacité maximale de rétention assurée par les actifs ou par la perte financière la plus importante à laquelle la société pourrait faire face sans se déclarer en faillite. Il convient de soumettre raisonnablement à essai la RBC estimée dans le cadre de scénarios d'essais de contraintes afin de fournir un niveau de confiance fiable. Le goût du risque d'une organisation reflète la volonté de la direction à utiliser sa RBC.
- ALARP/ALARA et SFAIRP: dans certaines juridictions, les critères prévus par la loi pour traiter le risque lié à la sécurité impliquent de s'assurer que le risque de blessure ou de mauvais état de santé soit aussi faible que raisonnablement réalisable (ALARP – *as low as is reasonably practicable*), aussi faible que raisonnablement possible (ALARA – *as low as reasonably achievable*) ou de démontrer que les moyens de maîtrise réduisent le plus possible le risque pour autant que cela soit raisonnablement réalisable (SFAIRP – *so far as is reasonably practicable*) (voir B.8.2);
- Globalement au moins équivalent (GAME) [1]: il est jugé acceptable que les risques aux conséquences néfastes provenant d'une source particulière augmentent s'il peut être démontré que les risques provenant d'autres sources ont diminué dans une mesure équivalente ou supérieure.

- Les critères coûts/bénéfices, comme le prix par vie sauvée ou le retour sur investissement (RSI).

6.1.6.3 Critères d'évaluation de l'importance d'un risque

Les critères de risque (termes de référence en fonction desquels est déterminée l'importance d'un risque) peuvent être formulés de manière à faire appel à l'une des caractéristiques et mesures du risque établies en 6.3.5 et en 6.3.7. Les considérations éthiques, culturelles, juridiques, sociales, de réputation, environnementales, contractuelles, financières, entre autres, peuvent également être pertinentes.

Une évaluation de l'importance d'un risque comparé à d'autres risques repose souvent sur une estimation de l'ampleur du risque comparée aux critères directement liés à des seuils établis en fonction des objectifs de l'organisation. La comparaison avec ces critères peut informer l'organisation des risques sur lesquels il convient de porter l'attention pour le traitement, en fonction de l'aptitude de ces risques à produire des résultats qui sortent des limites fixées pour les objectifs.

L'ampleur du risque est rarement le seul critère pertinent pour la prise de décision concernant l'importance du risque. D'autres facteurs pertinents peuvent inclure la durabilité (par exemple, la triple performance) et la résilience, les critères éthiques et juridiques, l'efficacité des moyens de maîtrise, l'impact maximal en cas d'absence ou de défaillance des moyens de maîtrise, la durée des conséquences, les coûts des moyens de maîtrise et les points de vue des parties prenantes.

Les techniques d'évaluation de l'importance d'un risque sont décrites à l'Article B.8.

6.1.6.4 Critères de choix entre des options

Une organisation est confrontée à de nombreuses décisions pour atteindre plusieurs objectifs, souvent contradictoires, et se retrouve en position de trouver un équilibre entre d'éventuels résultats néfastes et d'éventuels bénéfices. Pour prendre ce type de décision, il peut être nécessaire de respecter plusieurs critères et de trouver un compromis entre des objectifs contradictoires. Il convient d'identifier les critères pertinents pour la prise de décision, et de décider et considérer la mesure dans laquelle les critères doivent être pondérés ou des compromis consentis, les informations étant consignées dans un rapport et partagées. Lors de la définition des critères, il convient de tenir compte du fait que les coûts et les bénéfices peuvent varier d'une partie prenante à l'autre. Il convient de décider de quelle manière les différentes formes d'incertitude doivent être prises en considération.

Les techniques de l'Article B.9 portent sur le choix entre les différentes options.

6.2 Gestion des informations et développement de modèles

6.2.1 Généralités

Avant et pendant une appréciation du risque, il convient d'obtenir les informations pertinentes. Ces informations contribuent aux analyses statistiques, modèles ou techniques décrits à l'Annexe A et à l'Annexe B. Dans certains cas, les décideurs peuvent utiliser les informations sans analyse supplémentaire.

Les informations nécessaires à chaque stade dépendent des résultats de la collecte préalable d'informations, de l'objet et du domaine d'application de l'appréciation, ainsi que de la ou des méthodes à utiliser pour l'analyse. Il convient de décider de la manière dont les informations doivent être collectées, archivées et mises à disposition.

Il convient de décider des enregistrements des résultats de l'appréciation qui sont à conserver, ainsi que des enregistrements à générer, archiver, mettre à jour et fournir aux personnes qui pourraient en avoir besoin. Il convient de toujours indiquer les sources d'informations.

6.2.2 Collecte d'informations

Les informations peuvent être collectées à partir de sources comme des revues documentaires, des observations et des avis d'experts. Les données peuvent être collectées ou déduites, par exemple, de mesurages, d'expériences, d'entretiens et d'enquêtes.

En règle générale, les données représentent directement ou indirectement les pertes ou bénéfices passés. Des exemples incluent les échecs ou réussites d'un projet, le nombre de plaintes déposées, les profits ou pertes financiers, l'impact sur la santé, les blessures et décès, etc. Des informations supplémentaires peuvent également être disponibles, comme les causes de l'échec ou de la réussite, les sources de plaintes déposées, la nature des blessures, etc. Les données peuvent également inclure le résultat des modèles ou d'autres techniques d'analyse.

Il convient de décider de ce qui suit:

- la source d'informations et sa fiabilité;
- le type (s'il s'agit d'informations qualitatives et/ou quantitatives (voir 6.3.7.1), par exemple);
- le niveau (stratégique, tactique, opérationnel, par exemple);
- la quantité et la qualité des données nécessaires;
- la méthode de collecte;
- le niveau de confidentialité.

Si les données à analyser proviennent d'un échantillonnage, il convient d'établir la fiabilité statistique exigée, de manière à collecter des données suffisantes. Si aucune analyse statistique n'est nécessaire, il convient de l'indiquer.

Si des données ou résultats provenant d'appréciations précédentes sont disponibles, il convient d'établir en premier lieu si le contexte a évolué et, si c'est le cas, si les précédentes données ou précédents résultats restent pertinents.

Il convient d'évaluer la validité, la fiabilité et les limites des informations à utiliser dans l'appréciation, en tenant compte:

- de l'âge et de la pertinence des informations;
- de la source d'informations et des méthodes utilisées pour les collecter;
- des incertitudes et lacunes des informations;
- de l'autorité ou de la provenance des informations, ensembles de données, algorithmes et modèles.

6.2.3 Analyse des données

L'analyse des données peut fournir:

- une compréhension des conséquences antérieures et de leur vraisemblance à apprendre par l'expérience;
- les tendances générales, y compris les périodicités, qui donnent une indication de ce qui peut influencer l'avenir;
- les corrélations qui peuvent donner des indications sur les éventuels liens de causalité pour une validation ultérieure.

Il convient d'identifier et de comprendre les limites et les incertitudes.

Il ne peut pas être admis par hypothèse que les données passées s'appliqueront encore à l'avenir, mais elles peuvent renseigner les décideurs sur ce qui est plus ou moins susceptible de se produire dans le futur.

6.2.4 Développement et application des modèles

6.2.4.1 General

Un modèle est une représentation approximative de la réalité. Il a pour objet de transformer ce qui peut être une situation par nature complexe en termes plus simples, qui peuvent être analysés plus aisément. Il peut être utilisé pour aider à comprendre la signification des données et simuler ce qui pourrait se produire dans la pratique dans différentes conditions. Un modèle peut être physique, représenté dans un logiciel ou être un ensemble de relations mathématiques.

En règle générale, la modélisation comprend les étapes suivantes:

- description du problème;
- description de l'objectif de la génération d'un modèle et des résultats souhaités;
- développement d'un modèle conceptuel du problème;
- génération d'une représentation physique, logicielle ou mathématique du modèle conceptuel;
- développement de logiciels ou d'autres outils d'analyse des comportements du modèle;
- traitement des données;
- validation ou étalonnage du modèle par revue des résultats correspondant à des situations connues;
- établissement de conclusions à partir du modèle sur le problème dans le monde réel.

Chacune de ces étapes peut impliquer des approximations, des hypothèses et un avis d'expert, et il convient (dans la mesure du possible) que des personnes indépendantes des développeurs les valident. Il convient de revoir les hypothèses critiques en fonction des informations disponibles pour apprécier leur crédibilité.

Pour obtenir des résultats fiables lors de l'utilisation de modèles, il convient de valider ce qui suit:

- le modèle conceptuel représente de manière adéquate la situation en cours d'appréciation;
- le modèle est utilisé dans les limites contextuelles pour lesquelles il a été conçu;
- les concepts théoriques qui sous-tendent le modèle et tous les calculs associés sont bien compris;
- le choix des paramètres et des représentations mathématiques du concept est solide;
- la théorie mathématique qui sous-tend les calculs est bien comprise;
- les données d'entrée sont précises et fiables ou la nature du modèle tient compte de la fiabilité des données d'entrée utilisées;
- le modèle fonctionne comme prévu sans erreurs internes ni bogues;
- le modèle est stable et peu sensible aux faibles variations des principales entrées.

Cela peut être obtenu:

- en procédant à une analyse de sensibilité du modèle aux variations des paramètres d'entrée;
- en soumettant le modèle à des essais de contrainte avec des scénarios particuliers, souvent extrêmes;

- en comparant les résultats avec des données passées (autres que celles à partir desquelles le modèle a été développé);
- en vérifiant que des résultats similaires sont obtenus lorsque le modèle est exécuté par des personnes différentes;
- en vérifiant les résultats par rapport aux performances réelles.

Il convient que le modèle, ainsi que les théories et hypothèses sur lesquelles il s'appuie, soient accompagnés d'une documentation exhaustive et suffisante pour valider le modèle.

6.2.4.2 Utilisation de logiciels d'analyse

Des programmes logiciels peuvent être utilisés pour représenter et organiser les données ou pour les analyser. Les programmes logiciels utilisés pour la modélisation et l'analyse offrent souvent une simple interface utilisateur et donnent un résultat rapide, mais ces caractéristiques peuvent conduire à des résultats non valides que l'utilisateur ne remarque pas. Des résultats non valides peuvent être obtenus à cause:

- de lacunes dans les algorithmes utilisés pour représenter la situation;
- d'hypothèses formulées en matière de conception et d'utilisation du modèle qui sous-tend le logiciel;
- d'erreurs de saisie des données, y compris d'une mauvaise compréhension de leur signification;
- de problèmes de conversion de données lorsqu'un nouveau logiciel est utilisé;
- d'une mauvaise interprétation des résultats.

Les logiciels commerciaux sont souvent des boîtes noires (secret commercial) et peuvent contenir toutes ces erreurs.

Il convient de soumettre à essai les nouveaux logiciels en utilisant un modèle simple avec des entrées dont la sortie est connue, avant de passer à des essais de modèles plus complexes. Il convient de conserver les détails des essais pour les utiliser dans les mises à jour des versions ultérieures ou pour les nouveaux programmes d'analyse logicielle.

Les erreurs du modèle construit peuvent être vérifiées en augmentant ou diminuant une valeur d'entrée pour déterminer si la sortie répond comme prévu. Cela peut être appliqué à chacune des différentes entrées. Les erreurs d'entrée de données sont souvent identifiées en faisant varier les entrées de données. Cette approche donne également des informations relatives à la sensibilité du modèle aux variations des données.

Il est recommandé de bien comprendre les éléments mathématiques pertinents pour l'analyse particulière afin d'éviter les conclusions erronées. Non seulement les erreurs ci-dessus sont probables, mais le choix d'un programme particulier peut également ne pas être approprié. Il est aisé de suivre un programme et de prendre pour hypothèse que la réponse est par conséquent exacte. Il convient de rassembler les preuves permettant de vérifier que les résultats sont raisonnables.

6.3 Application des techniques d'appréciation du risque

6.3.1 Vue d'ensemble

Les techniques décrites à l'Annexe A et à l'Annexe B sont utilisées pour mieux comprendre un risque comme élément d'informations nécessaire à la prise de décision en cas d'incertitude, y compris les décisions relatives à l'éventuel traitement du risque et à la manière de l'appliquer.

Les techniques d'appréciation peuvent être utilisées pour:

- identifier le risque (voir 6.3.2);

- déterminer les causes, les sources et les facteurs de risque, ainsi que le niveau d'exposition à ce risque (voir 6.3.3);
- examiner l'efficacité globale des moyens de maîtrise, et de l'effet modificateur des traitements du risque suggérés (voir 6.3.4);
- comprendre les conséquences et la vraisemblance (voir 6.3.5);
- analyser les interactions et les dépendances (voir 6.3.6);
- fournir une mesure du risque (voir 6.3.7).

Les facteurs à prendre en compte lors du choix d'une technique particulière pour ces activités sont décrits à l'Article 7.

En règle générale, l'analyse peut être descriptive (rapport d'une revue documentaire, analyse de scénario ou description de conséquences, par exemple) ou quantitative, lorsque les données sont analysées pour générer des valeurs numériques. Dans certains cas, des échelles de classement peuvent être appliquées pour comparer des risques particuliers.

Il convient que la manière d'apprécier un risque et la forme du résultat soient compatibles avec tous les critères définis. Par exemple, des critères quantitatifs exigent une technique d'analyse quantitative qui produit un résultat avec les unités appropriées.

Il convient d'utiliser des opérations mathématiques uniquement si les métriques choisies le permettent. En règle générale, il convient de ne pas utiliser d'opérations mathématiques avec les échelles ordinales. Même avec une analyse totalement quantitative, les valeurs d'entrée sont souvent des estimations. Il convient de ne pas attribuer aux résultats un niveau d'exactitude et de précision supérieur à celui correspondant aux données et méthodes utilisées.

6.3.2 Identification du risque

L'identification du risque permet une prise en compte explicite de l'incertitude. Toutes les sources d'incertitudes et les effets tant bénéfiques que néfastes peuvent être pertinents, en fonction du contexte et du domaine d'application de l'appréciation.

Les techniques d'identification du risque s'appuient en général sur les connaissances et l'expérience d'un certain nombre de parties prenantes (voir B.1.1). Il s'agit notamment de savoir:

- quelle incertitude existe et quels peuvent être ses effets;
- quelles circonstances ou quels problèmes (tangibles ou intangibles) sont susceptibles de présenter des conséquences futures;
- quelles sources de risques sont présentes ou peuvent apparaître;
- quels moyens de maîtrise sont en place et s'ils sont efficaces;
- quels événements et conséquences peuvent se produire, et comment, quand, où et pourquoi;
- ce qu'il s'est passé et comment cela peut être raisonnablement associé au futur;
- quels aspects humains et facteurs organisationnels pourraient s'appliquer.

Des enquêtes physiques peuvent également être utiles pour identifier les sources de risques ou les signes précurseurs d'éventuelles conséquences.

Le résultat de l'identification du risque peut être consigné sous la forme d'une liste de risques avec les événements, les causes et les conséquences spécifiés, ou en utilisant d'autres formats.

Quelles que soient les techniques utilisées, il convient d'appréhender l'identification des risques de manière méthodique et itérative de sorte qu'elle soit complète et efficace. Il convient dans la mesure du possible d'identifier le risque suffisamment tôt pour permettre la prise de mesures. Il arrive cependant que certains risques ne puissent pas être identifiés au cours d'une appréciation du risque. Il convient donc de mettre en place un mécanisme pour recueillir les risques émergents et reconnaître les signes précurseurs d'une réussite ou d'un échec potentiel(le).

Les techniques d'identification du risque sont présentées à l'Article B.2.

6.3.3 Détermination des sources, des causes et des facteurs de risque

L'identification des causes, des sources et des facteurs de risque peut:

- contribuer à estimer la vraisemblance d'un événement ou d'une conséquence;
- aider à identifier les traitements qui vont modifier le risque;
- aider à déterminer les indicateurs précurseurs et leurs seuils de détection;
- déterminer les causes communes qui peuvent aider à développer des priorités de traitement du risque.

Les sources de risques peuvent inclure des événements, des décisions, des actions et des processus, aussi bien favorables que défavorables, ainsi que des situations dont l'existence est connue, mais où les conséquences sont incertaines. Toute forme d'incertitude décrite en 4.1 peut être une source de risque.

Les événements et conséquences peuvent avoir plusieurs causes ou chaînes de causalité.

Le risque ne peut souvent être maîtrisé qu'en modifiant les facteurs de risque. Ces facteurs ont un impact sur l'état et l'évolution des expositions au risque, et affectent souvent plusieurs risques. Par conséquent, il est souvent nécessaire de prêter une plus grande attention aux sources de risques individuels.

Les techniques permettant de déterminer les sources, les causes et les facteurs de risque sont décrites à l'Article B.3.

6.3.4 Examen de l'efficacité des moyens de maîtrise existants

Le risque est affecté par l'efficacité globale des moyens de maîtrise en place. Il convient de prendre en considération les aspects suivants des moyens de maîtrise:

- le mécanisme selon lequel les moyens de maîtrise sont destinés à agir pour modifier le risque;
- si les moyens de maîtrise sont en place, en mesure de fonctionner comme prévu et permettent d'obtenir les résultats prévus;
- si la conception des moyens de maîtrise présente des faiblesses ou la manière dont les moyens de maîtrise sont appliqués;
- si les moyens de maîtrise présentent des lacunes;
- si les moyens de maîtrise fonctionnent de manière indépendante ou s'il est nécessaire qu'ils fonctionnent de manière collective pour être efficaces;
- s'il existe des facteurs, des conditions, des vulnérabilités ou des circonstances qui peuvent réduire ou éliminer l'efficacité des moyens de maîtrise, y compris les défaillances de cause commune;
- si les moyens de maîtrise eux-mêmes génèrent des risques supplémentaires.

NOTE Un risque peut avoir plusieurs moyens de maîtrise et les moyens de maîtrise peuvent affecter plusieurs risques.

Il convient de faire une distinction entre les moyens de maîtrise qui modifient la vraisemblance et/ou les conséquences et les moyens de maîtrise qui modifient la répartition du risque entre les parties prenantes. Par exemple, l'assurance et les autres formes de financement du risque n'ont pas d'impact direct sur la vraisemblance d'un événement ou sur ses résultats, mais peuvent rendre certaines conséquences plus tolérables pour une partie prenante particulière en réduisant leur étendue ou en lissant les flux de trésorerie.

Dans la mesure du possible, il convient de valider toutes les hypothèses formulées lors de l'analyse du risque concernant les effets et la fiabilité réels des moyens de maîtrise en mettant particulièrement l'accent sur les moyens de maîtrise individuels ou combinés qui sont admis comme ayant un effet modificateur important. Il convient de prendre en considération les informations recueillies grâce à une surveillance de routine et à une revue des moyens de maîtrise.

Les techniques d'analyse des moyens de maîtrise sont décrites à l'Article B.4.

6.3.5 Compréhension des conséquences et de la vraisemblance

6.3.5.1 Analyse du type, de l'ampleur et de la durée des conséquences

L'analyse des conséquences peut s'étendre d'une simple description des résultats à une modélisation quantitative ou une analyse de vulnérabilité approfondie. Il convient de prendre en considération les effets collatéraux (effets domino ou secondaires), lorsqu'une conséquence découle d'une autre.

Le risque peut être associé à un certain nombre de types de conséquences différents, qui ont un impact sur les différents objectifs. Il convient de choisir les types de conséquences à analyser au moment de la planification de l'appréciation. Il convient de vérifier les déclarations de contexte afin de s'assurer que les conséquences à analyser correspondent bien aux objectifs de l'appréciation et aux décisions à prendre. Cela peut être adapté au fil de l'appréciation à mesure de la disponibilité d'informations supplémentaires.

L'ampleur des conséquences peut être exprimée de manière quantitative sous la forme d'une valeur ponctuelle ou d'une répartition. Une répartition peut être appropriée lorsque:

- la valeur correspondant à la conséquence est incertaine;
- les conséquences varient en fonction des circonstances;
- les paramètres ayant un impact sur les conséquences varient.

La prise en compte de l'ensemble de la répartition liée à une conséquence donne des informations exhaustives. Il est possible de résumer la répartition sous la forme d'une valeur ponctuelle, comme la valeur prévue (moyenne), la variation (variance) ou le pourcentage en bout ou dans une autre partie pertinente de la répartition (centile).

Quelle que soit la méthode d'obtention d'une valeur ponctuelle ou de valeurs permettant de représenter une répartition des conséquences, il existe des hypothèses sous-jacentes et des incertitudes relatives:

- à la forme de la distribution choisie pour ajuster les données (continue ou discrète, normale ou asymétrique, par exemple);
- au moyen le plus approprié de représenter cette répartition sous la forme d'une valeur ponctuelle;
- à la valeur de l'estimation ponctuelle, compte tenu des incertitudes inhérentes aux données à partir desquelles la répartition a été générée.

Il convient de ne pas prendre pour hypothèse que les données relatives au risque suivent nécessairement une répartition normale.

Dans certains cas, les informations peuvent être résumées sous la forme de classements qualitatifs ou semi-quantitatifs, qui peuvent être utilisés pour comparer les risques.

L'ampleur des conséquences peut également varier en fonction d'autres paramètres. Par exemple, les conséquences sur la santé d'une exposition à un produit chimique dépendent en général de la dose à laquelle la personne ou d'autres espèces ont été exposées. Dans cet exemple, le risque est en général représenté par une courbe dose-effet qui décrit la probabilité d'une issue particulière (la mort, par exemple) en fonction d'une dose à court terme ou cumulée.

Les conséquences peuvent également varier dans le temps. Par exemple, plus une défaillance dure longtemps, plus ses effets néfastes peuvent s'aggraver. Il convient que les techniques appropriées en tiennent compte.

Les conséquences sont parfois le résultat d'expositions à plusieurs sources de risques: par exemple, effets sur l'environnement ou la santé après une exposition à des sources de risques biologiques, chimiques, physiques et psychosociales. Lors de l'évaluation de telles expositions multiples, il convient de tenir compte également de la possibilité d'effets synergiques, ainsi que de l'influence de la durée et de l'étendue de l'exposition.

6.3.5.2 Analyse de vraisemblance

La vraisemblance peut faire référence à la vraisemblance d'un événement ou à celle d'une conséquence spécifiée. Il convient d'établir explicitement le paramètre auquel s'applique une valeur de vraisemblance et il convient de définir précisément l'événement ou la conséquence dont la vraisemblance est en train d'être établie. Pour définir la vraisemblance de manière exhaustive, il peut être nécessaire d'inclure une déclaration concernant l'exposition et la durée.

La vraisemblance peut être décrite de différentes manières, notamment sous la forme d'une probabilité ou d'une fréquence attendue, ou bien dans des termes descriptifs (par exemple, "très probable"). Lorsqu'un terme descriptif est utilisé, il convient d'en définir la signification. La vraisemblance peut être associée à une incertitude, laquelle peut être représentée sous la forme d'une distribution de valeurs reflétant le degré de croyance quant à l'occurrence d'une valeur particulière.

Si un pourcentage est utilisé comme mesure de la vraisemblance, il convient de préciser la nature du rapport auquel le pourcentage s'applique.

EXEMPLE 1 La déclaration selon laquelle un fournisseur a 5 % de chance de ne pas assurer une livraison est vague tant en ce qui concerne la période de temps que la population. Il n'apparaît pas clairement non plus si le pourcentage concerne 5 % des projets ou 5 % des fournisseurs. Pour être plus explicite, la déclaration serait formulée de la manière suivante: "la probabilité qu'un ou que plusieurs fournisseurs n'assurent pas la livraison des marchandises ou des services exigés pendant la durée d'un projet est de 5 % des projets".

Pour réduire le plus possible les mauvaises interprétations lors de l'expression d'une vraisemblance, de manière qualitative ou quantitative, il convient de préciser explicitement la période de temps et la population concernée dans le domaine d'application de l'appréciation.

EXEMPLE 2 La probabilité qu'un ou que plusieurs fournisseurs n'assurent pas la livraison des marchandises ou des services exigés par un projet dans les deux mois qui suivent est de 1 % des projets, alors que sur une période de six mois, une défaillance peut se produire dans 3 % des projets.

De nombreux partis pris peuvent avoir un impact sur les estimations de vraisemblance. De plus, l'interprétation de l'estimation de vraisemblance peut être différente selon le contexte dans lequel elle a été établie. Il convient de veiller à bien comprendre les éventuels effets des partis pris individuels (cognitifs) et culturels.

Les techniques permettant de comprendre les conséquences et la vraisemblance sont décrites à l'Article B.5.

6.3.6 Analyse des interactions et des dépendances

Il existe en général de nombreuses interactions et dépendances entre les risques. Par exemple, une seule cause peut avoir plusieurs conséquences ou une conséquence particulière peut avoir plusieurs causes. L'occurrence de certains risques peut rendre celle d'autres risques plus ou moins probable, ces liens de causalité pouvant donner des résultats en cascade ou en boucle.

Pour procéder à une appréciation du risque plus fiable lorsque les liens de causalité entre les risques sont importants, il peut s'avérer utile de créer un modèle causal qui intègre les risques sous certaines formes. Des thèmes communs peuvent être déterminés dans les informations relatives au risque (causes communes, facteurs de risque communs ou résultats communs, par exemple).

Les interactions entre les risques peuvent avoir un ensemble d'impacts sur la prise de décision (l'importance croissante des activités couvrant plusieurs risques connexes ou l'augmentation de l'attrait d'une option sur d'autres, par exemple). Les risques peuvent être susceptibles d'être traités en commun ou, dans certaines situations, le traitement d'un risque peut avoir des implications positives ou négatives ailleurs. Les actions de traitement peuvent parfois être regroupées de manière à réduire considérablement la quantité de travail et à équilibrer plus efficacement les ressources disponibles. Il convient qu'un plan de traitement coordonné tienne compte de ces facteurs plutôt que de prendre pour hypothèse qu'il convient de traiter chaque risque de manière indépendante.

Les techniques d'analyse des interactions et des dépendances sont décrites à l'Article B.6.

6.3.7 Compréhension des mesures du risque

6.3.7.1 Détermination des mesures du risque

Dans certaines situations, il est utile de mesurer le risque en combinant l'ampleur des conséquences éventuelles et la vraisemblance de ces conséquences. Cela peut impliquer de procéder à des mesures qualitatives, semi-quantitatives ou quantitatives.

- Les approches qualitatives reposent en général sur des échelles descriptives (nominales) ou de classement (ordinales) pour les conséquences et les vraisemblances.
- Les approches semi-quantitatives se caractérisent par:
 - un paramètre (en général la vraisemblance) exprimé de manière quantitative et un autre décrit ou exprimé sur une échelle de classement;
 - des échelles divisées en bandes discrètes dont les limites sont exprimées de manière quantitative. Des points sont souvent tracés sur l'échelle de manière à produire une relation logarithmique pour correspondre aux données;
 - des descripteurs numériques ajoutés aux points d'échelle, dont la signification est décrite de manière qualitative.

L'utilisation d'échelles semi-quantitatives peut donner lieu à de mauvaises interprétations si la base des calculs n'est pas soigneusement expliquée. Il convient donc de valider les approches semi-quantitatives et de les utiliser avec précaution.

- Les approches quantitatives s'appuient sur des mesures de conséquences et de vraisemblances exprimées sur des échelles numériques (de rapport). Lorsqu'un risque est analysé en termes quantitatifs, il convient de s'assurer que les unités et dimensions appropriées sont utilisées et reprises tout au long de l'appréciation.

Les techniques qualitatives et semi-quantitatives peuvent être utilisées uniquement pour comparer des risques à d'autres risques mesurés de la même manière ou avec des critères exprimés de la même façon. Elles ne peuvent pas être utilisées pour combiner ou agréger directement des risques, et sont très difficiles à utiliser dans des situations où les conséquences sont à la fois positives et négatives ou lorsque des compromis doivent être trouvés entre les risques.

Si les estimations quantitatives d'une conséquence et de sa vraisemblance sont combinées sous la forme d'un simple produit pour déterminer l'ampleur d'un risque, il peut y avoir une perte d'informations. Aucune distinction n'est notamment établie entre les risques aux conséquences importantes et dont la vraisemblance est faible et les risques aux conséquences mineures qui se produisent souvent. Pour compenser cette absence de distinction, un facteur de pondération peut être appliqué à la conséquence ou à la vraisemblance, auquel cas il convient d'utiliser cette technique avec précaution.

Les risques ne peuvent pas toujours être décrits ou estimés de manière appropriée par une seule valeur représentant la vraisemblance d'une conséquence particulière. Des exemples d'applications incluent les situations dans lesquelles:

- les conséquences sont mieux exprimées sous la forme d'une distribution de probabilité des conséquences;
- un événement présente un certain nombre de causes différentes ou donne lieu à un ensemble de résultats et d'effets collatéraux possibles;
- les conséquences surviennent conjointement à la suite d'une exposition continue à une source de risque;
- les sources de risques (problèmes systémiques, par exemple) sont identifiables, mais il est très difficile de spécifier la nature et/ou la vraisemblance des conséquences qui peuvent survenir (dans ce cas, il devient impossible d'estimer une ampleur valable du risque en termes de vraisemblance et de conséquence).

Lorsqu'un risque a une distribution de conséquences possibles, une mesure du risque peut être obtenue en calculant la moyenne pondérée de probabilité des conséquences (c'est-à-dire la valeur attendue). Ceci peut cependant ne pas toujours produire une bonne mesure du risque, car le résultat reflète la moyenne des conséquences de la distribution. Cela conduit à une perte d'informations sur les conséquences moins probables, qui peuvent être graves et donc importantes pour la compréhension du risque. Les techniques de traitement des valeurs extrêmes ne sont pas incluses dans le présent document.

NOTE Une valeur attendue équivaut à la somme de chaque paire vraisemblance/conséquence sur une distribution, ce qui revient à utiliser la conséquence moyenne de la distribution.

Des exemples de mesures quantitatives de l'ampleur d'un risque sont:

- la fréquence d'occurrence prévue d'une conséquence déterminée (le nombre d'accidents de la route par milliers de kilomètres parcourus dans une région, par exemple);
- la durée prévue entre les événements considérés (la durée moyenne de disponibilité d'un élément, par exemple);
- la probabilité d'une issue spécifiée sur une période d'exposition définie (pertinente lorsque les conséquences s'accumulent sur une période d'exposition), comme la probabilité de contracter un cancer dans une vie à la suite d'une exposition à une dose définie de produits chimiques;
- une valeur prévue (rentabilité financière ou bénéfices financiers prévus sur une période d'investissement ou charge prévue qui pèse sur la santé publique en termes de coût par année de vie ajustée sur l'incapacité par million de personnes par an, par exemple);
- la représentation statistique de la forme d'une répartition des conséquences (la variance ou la volatilité des retours sur investissement, par exemple);
- une valeur supérieure, inférieure ou égale à un centile spécifié dans une distribution de conséquences;

EXEMPLE Le fait d'avoir 90 % de chance de réaliser un bénéfice dans le cadre d'un projet, ou la valeur en risque (VaR) d'un portefeuille qui mesure la perte éventuelle dans un portefeuille sur une période de temps spécifiée selon une probabilité définie.

- une mesure extrême associée à la distribution des conséquences (les conséquences maximales prévues, par exemple).

Les métriques reposant sur les conséquences (la perte crédible maximale ou la perte maximale probable, par exemple) sont essentiellement utilisées lorsqu'il s'avère difficile de définir quels moyens de maîtrise sont susceptibles d'être défaillants ou lorsque les données sur lesquelles reposent les estimations de vraisemblance sont insuffisantes.

L'ampleur du risque dépend des hypothèses formulées quant à la présence et à l'efficacité des moyens de maîtrise pertinents. Les professionnels utilisent souvent des termes comme "risque inhérent" ou "risque brut" (lorsque les moyens de maîtrise qui peuvent échouer sont censés l'avoir été) et "risque résiduel" ou "risque net" (correspondant au niveau d'un risque lorsque les moyens de maîtrise sont censés fonctionner comme prévu). Toutefois, il est difficile de définir ces termes de manière univoque, et il est donc conseillé de toujours établir explicitement les hypothèses formulées concernant les moyens de maîtrise.

Lors de la notification de l'ampleur d'un risque (de manière qualitative ou quantitative), il convient de décrire les incertitudes liées aux hypothèses et aux paramètres d'entrée et de sortie.

6.3.7.2 Agrégation des mesures du risque

Dans certains cas (une allocation de capital, par exemple), il peut être utile de combiner des valeurs pour un ensemble de risques afin de générer une seule valeur. En principe, les risques peuvent être combinés à condition d'être caractérisés par une seule conséquence, mesurée dans les mêmes unités (une valeur monétaire, par exemple). En d'autres termes, ils peuvent être uniquement combinés lorsque les conséquences et la vraisemblance sont établies de manière quantitative et que les unités sont cohérentes et correctes. Dans certaines situations, une mesure d'utilité peut faire office d'échelle commune pour quantifier et combiner des conséquences mesurées dans différentes unités.

Des informations relatives aux risques du composant sont perdues lors du développement d'une seule valeur consolidée pour un ensemble de risques plus complexes. De plus, à moins de prendre toutes les précautions, la valeur consolidée peut être imprécise et éventuellement trompeuse. Toutes les méthodes d'agrégation des risques en une seule valeur font l'objet d'hypothèses sous-jacentes qu'il convient de bien comprendre avant d'être appliquées. Il convient d'analyser les données pour rechercher les corrélations et les dépendances ayant un impact sur la manière de combiner les risques. Il convient qu'une analyse de scénario et des essais de contrainte viennent à l'appui des techniques de modélisation utilisées pour générer un niveau de risque agrégé.

Si les modèles intègrent des calculs impliquant des répartitions, il convient qu'ils contiennent des corrélations entre ces distributions de manière appropriée. Si les corrélations ne sont pas correctement prises en considération, les résultats sont imprécis et peuvent être très trompeurs. La consolidation de risques en les additionnant simplement n'est pas une base fiable de prise de décision et peut donner lieu à des résultats non souhaitables. La simulation de Monte-Carlo peut être utilisée pour combiner des distributions (voir B.5.10).

Les mesures qualitatives ou semi-quantitatives du risque ne peuvent pas être directement agrégées. De même, seules des déclarations qualitatives générales peuvent être formulées concernant l'efficacité relative des moyens de maîtrise en fonction des mesures qualitatives ou semi-quantitatives de variations de niveau de risque.

Les données pertinentes relatives à différents risques peuvent être rassemblées de différentes manières pour aider les décideurs. Il est possible de procéder à une agrégation qualitative reposant sur des avis d'expert en s'appuyant sur des informations de risque plus précises. Il convient d'énoncer clairement les hypothèses formulées, ainsi que les informations utilisées pour procéder à des agrégations qualitatives du risque.

6.3.7.3 Risque sociétal

Lorsqu'une population est exposée à un risque, une simple agrégation de chaque niveau de risque en procédant à une multiplication par la population exposée ne représente pas convenablement, dans la plupart des cas, le véritable impact des conséquences. Par exemple, il peut être nécessaire de prendre en considération différemment le risque d'accident mortel pour un individu à la suite d'un événement (comme une rupture de barrage) du même événement ayant un impact sur un groupe d'individus.

Le risque sociétal est souvent exprimé et évalué par la relation entre la fréquence d'occurrence d'une conséquence (F) et le nombre de personnes qui supportent les conséquences (N) (voir diagrammes F-N en B.8.3).

Les techniques utilisées pour produire une mesure du risque sont décrites à l'Article B.7.

6.4 Examen de l'analyse

6.4.1 Vérification et validation des résultats

Dans la mesure du possible, il convient de vérifier et de valider les résultats de l'analyse. La vérification implique de s'assurer que l'analyse a été correctement réalisée. Elle implique également de s'assurer que la bonne analyse a été réalisée pour atteindre les objectifs exigés. Dans certaines situations, la vérification et la validation peuvent impliquer des processus d'examen indépendants.

La validation peut consister à:

- vérifier la pertinence du domaine d'application de l'analyse pour les objectifs indiqués;
- revoir toutes les hypothèses critiques pour s'assurer de leur crédibilité à la lumière des informations disponibles;
- vérifier que les méthodes, modèles et données appropriés ont été utilisés;
- utiliser plusieurs méthodes, approximations et analyses de sensibilité pour soumettre à essai et valider les conclusions.

La vérification peut consister à:

- vérifier la validité des manipulations et calculs mathématiques;
- vérifier que les résultats ne sont pas sensibles à la manière dont les données ou les résultats sont affichés ou présentés;
- comparer les résultats avec ceux de l'expérience passée si des données existent ou en comparant les résultats après leur survenue;
- établir si les résultats sont sensibles à la manière d'afficher ou de présenter les données ou les résultats, et à identifier les paramètres d'entrée ayant un impact important sur les résultats de l'appréciation;
- comparer les résultats avec ceux d'une expérience passée ou acquise, y compris l'obtention de commentaires explicites au fil du temps.

6.4.2 Analyse d'incertitude et de sensibilité

Il convient que cette analyse du risque permette de comprendre les incertitudes dans l'analyse et d'apprécier ce qu'elles impliquent en matière de fiabilité des résultats. Il convient de toujours communiquer les incertitudes et leurs implications aux décideurs.

L'incertitude des résultats d'analyse peut provenir:

- d'une variabilité du système à l'étude;

- de données issues d'une source non fiable ou de données incohérentes ou insuffisantes (le type de données collectées ou les méthodes de collecte peuvent avoir changé, par exemple);
- d'une ambiguïté (manière dont les descripteurs qualitatifs sont établis ou compris, par exemple);
- de la méthode d'analyse qui ne représente pas convenablement la complexité du système;
- d'une grande dépendance des personnes à l'égard des avis ou jugements d'experts;
- de données pertinentes qui peuvent ne pas exister ou d'une organisation qui n'a pas collecté les données nécessaires;
- de données passées qui peuvent ne pas être une base fiable sur laquelle prédire l'avenir, un élément dans le contexte ou les circonstances ayant changé;
- d'incertitudes ou d'approximations dans les hypothèses formulées.

Si l'analyse révèle un manque de données fiables, il convient dans la mesure du possible de collecter d'autres données. Cela peut impliquer de mettre en œuvre de nouveaux mécanismes de surveillance. D'autre part, il convient d'ajuster le processus d'analyse de manière à tenir compte de l'insuffisance de données.

Une analyse de sensibilité peut être réalisée afin d'évaluer l'importance des incertitudes dans les données ou dans les hypothèses sous-jacentes à l'analyse. L'analyse de sensibilité implique de déterminer la modification relative des résultats due à des modifications de paramètres d'entrée individuels. Elle permet de distinguer les données qui ont besoin d'être précises, de celles qui sont moins sensibles et dont les effets sur l'exactitude générale sont par conséquent moins importants. Il convient de définir les paramètres auxquels l'analyse est sensible et le degré de sensibilité, selon le cas.

Il convient d'identifier les paramètres essentiels pour l'appréciation et qui font l'objet de modifications pour surveillance continue, de manière à pouvoir mettre à jour l'appréciation du risque et, le cas échéant, reconsidérer les décisions.

6.4.3 Surveillance et revue

La surveillance peut permettre:

- de comparer les résultats réels à ceux prévus par l'appréciation du risque et, ainsi, améliorer les appréciations futures;
- de rechercher des précurseurs et des indicateurs précurseurs de conséquences potentielles qui ont été identifiées par l'appréciation;
- de collecter les données nécessaires à une bonne compréhension du risque;
- de rechercher de nouveaux risques et des changements imprévus qui peuvent révéler un besoin de mettre à jour l'appréciation.

Si une analyse de sensibilité indique des paramètres d'importance particulière pour le résultat d'une analyse, il convient également d'en tenir compte pour la surveillance.

Il convient de revoir régulièrement les appréciations pour identifier si une modification a eu lieu, y compris celle d'un contexte ou d'une hypothèse, et si de nouvelles informations ou méthodes sont disponibles.

6.5 Application des résultats à l'appui des décisions

6.5.1 Vue d'ensemble

Les résultats de l'analyse du risque fournissent des éléments d'informations nécessaires pour les décisions à prendre et les actions exécutées.

NOTE Une compréhension du risque peut fournir des éléments d'informations nécessaires aux actions, même lorsqu'aucun processus décisionnel explicite n'est appliqué.

Lors de l'établissement du contexte de l'appréciation, il convient d'avoir défini les facteurs à prendre en considération lors de la prise de décision ainsi que tous les critères spécifiques (voir 6.1.6).

Deux types de décisions peuvent être distingués:

- décisions relatives à l'importance du risque et à la nécessité et la manière de traiter le risque;
- décisions impliquant la comparaison d'options lorsque chacune fait l'objet d'incertitudes (laquelle des opportunités saisir, par exemple).

6.5.2 Décisions relatives à l'importance du risque

Les informations issues de l'identification et de l'analyse du risque peuvent être utilisées pour déterminer s'il convient d'accepter le risque et définir l'importance comparative du risque par rapport aux objectifs et aux seuils de performances de l'organisation. Cela contribue à la prise de décisions quant à savoir si le risque est acceptable ou s'il exige un traitement et toutes les priorités en la matière.

Certains risques peuvent être acceptés pour une durée déterminée (par exemple, pour laisser le temps de mettre en place des moyens de traitement). Il convient que l'évaluateur clarifie les mécanismes d'acceptation temporaire des risques et le processus à utiliser en vue d'un réexamen ultérieur.

Les priorités en matière de traitement, pour la surveillance ou pour une analyse plus approfondie, s'appuient souvent sur une ampleur du risque déterminée en combinant une conséquence représentative et sa vraisemblance, et sont affichées dans une matrice conséquence/vraisemblance (B.10.3). Cette méthode présente certaines limites (voir B.10.3.5 et 6.3.7.1). Les facteurs, autres que l'ampleur du risque, qui peuvent être pris en considération pour décider des priorités sont:

- les autres mesures associées au risque, comme les conséquences maximales ou prévues ou l'efficacité des moyens de maîtrise;
- les caractéristiques qualitatives des événements ou leurs conséquences possibles;
- les points de vue et perceptions des parties prenantes;
- le coût et la possibilité d'exécution d'autres traitements comparés aux améliorations obtenues;
- les interactions entre les risques, y compris les effets des traitements sur d'autres risques.

Lorsque les risques ont été évalués et les traitements choisis, le processus d'appréciation du risque peut être répété pour vérifier que les traitements suggérés n'ont pas généré d'autres risques néfastes et que le risque résiduel au terme du traitement se trouve dans les limites du goût du risque de l'organisation.

Les techniques d'évaluation de l'importance d'un risque sont décrites à l'Article B.8.

6.5.3 Décisions impliquant de choisir parmi des options

En principe, le choix parmi des options implique de peser les éventuels avantages et inconvénients de chacune d'elles, en tenant compte des incertitudes, notamment:

- des incertitudes associées aux éventuels résultats des options et aux estimations des coûts et des bénéfices;
- des éventuels événements et développements qui peuvent avoir un impact sur les résultats;

- des valeurs que les différentes parties prenantes placent sur les coûts et les avantages;
- de l'incertitude autour des jugements formulés à partir des résultats de l'analyse du risque, y compris l'évaluation du maintien ou non à terme des objectifs et des critères.

Ce type de décision s'appuie souvent sur le jugement d'experts fondé sur la compréhension acquise dans le cadre d'une analyse des options concernées et de la prise en compte du risque associé à chacune d'elles:

- des compromis qu'il peut être nécessaire de consentir entre les objectifs contradictoires;
- du goût du risque de l'organisation;
- des différentes attitudes et croyances des parties prenantes.

Les techniques pouvant être utilisées pour comparer les options qui impliquent des incertitudes sont décrites à l'Article B.9.

6.6 Enregistrement et consignation du processus d'appréciation du risque et de ses résultats

Il convient de documenter les résultats de l'appréciation du risque, les méthodologies utilisées et la justification des hypothèses retenue ainsi que toute recommandation, et de prendre une décision en ce qui concerne les informations à communiquer et les personnes à qui les communiquer. Il convient de définir la manière dont les enregistrements doivent être révisés et mis à jour.

Les enregistrements ont pour objet de:

- communiquer des informations relatives au risque aux décideurs et autres parties prenantes, notamment les organismes de réglementation;
- fournir un enregistrement et une justification de la prise de décision;
- conserver les résultats de l'appréciation pour un usage et une référence ultérieurs;
- suivre les performances et les tendances;
- s'assurer que les risques sont bien compris et gérés de manière appropriée;
- permettre une vérification de l'appréciation;
- fournir un journal d'audit.

Il convient par conséquent de fournir tous les documents ou enregistrements au moment opportun et sous une forme qui peut être comprise par ceux qui les lisent. Il convient également que les documents apportent l'expertise technique nécessaire pour la validation et qu'ils incluent des détails suffisants pour conserver l'appréciation pour un usage ultérieur. Il convient que les informations fournies soient suffisantes pour permettre, d'une part, le suivi des processus et, d'autre part, la revue et la validation des résultats. Il convient d'énoncer clairement les hypothèses formulées, les limites des données ou méthodes, ainsi que les raisons qui justifient les recommandations.

Il convient d'exprimer les risques en des termes compréhensibles, et que les unités dans lesquelles sont exprimées les mesures quantitatives soient claires et correctes.

Il convient que les personnes qui présentent les résultats caractérisent leur confiance ou celle de leur équipe en la précision et l'exhaustivité des résultats. Il convient de communiquer les incertitudes de manière adéquate de sorte que le rapport n'implique pas un niveau de certitude au-delà de la réalité.

Les techniques d'enregistrement et de consignation sont décrites à l'Article B.10.

7 Choix des techniques d'appréciation du risque

7.1 Généralités

L'Article 7 décrit les facteurs à prendre en considération lors du choix d'une ou de plusieurs techniques pour un objet particulier. Les Annexes A et B répertorient et expliquent plus en détail certaines techniques souvent utilisées. Elles décrivent les caractéristiques de chaque technique et l'éventail d'applications possibles, avec leurs forces et leurs faiblesses inhérentes.

A l'origine, la plupart des techniques décrites dans le présent document ont été développées pour des secteurs industriels particuliers en vue de gérer des types particuliers de résultats non souhaités. Plusieurs de ces techniques sont similaires, mais utilisent différentes terminologies, reflétant leur développement indépendant pour un objectif similaire dans différents secteurs. Au fil du temps, l'application de plusieurs de ces techniques a été élargie allant, par exemple, des applications d'ingénierie technique aux situations financières ou administratives ou pour prendre en compte les résultats tant positifs que négatifs. De nouvelles techniques ont vu le jour et les anciennes ont été adaptées aux nouvelles circonstances. Les techniques et leurs applications continuent d'évoluer. Une meilleure compréhension du risque est possible en utilisant ces techniques hors de leur application d'origine. Les Annexes A et B indiquent donc les caractéristiques des techniques qui peuvent être utilisées pour déterminer l'éventail des circonstances dans lesquelles elles peuvent être appliquées.

7.2 Choix des techniques

Il convient de définir et d'ajuster le choix de la technique et la manière de l'appliquer en fonction du contexte et de l'utilisation, et de donner des informations dont le type et la forme correspondent aux besoins des parties prenantes. En termes généraux, il convient de définir le nombre et le type de techniques choisies en fonction de l'importance de la décision et de tenir compte des contraintes de temps, d'autres ressources, ainsi que des coûts d'opportunité.

Pour décider si une technique qualitative ou quantitative est plus appropriée, le principal critère à prendre en considération est la forme des données de sortie la plus utile aux parties prenantes, ainsi que la disponibilité et la fiabilité des données. En règle générale, les techniques quantitatives exigent des données de très bonne qualité si elles doivent donner des résultats significatifs. Toutefois, dans certains cas, lorsque les données ne sont pas suffisantes, la rigueur nécessaire à l'application d'une technique quantitative peut permettre de mieux comprendre le risque, même si le résultat du calcul peut s'avérer incertain.

Un choix de techniques pertinent est souvent possible pour une circonstance donnée. Il peut être nécessaire de prendre en compte plusieurs techniques, dont l'application peut parfois apporter une compréhension supplémentaire utile. [2] Différentes techniques peuvent également être appropriées au fur et à mesure que des informations deviennent disponibles.

Au moment du choix d'une ou de plusieurs techniques, il convient donc de prendre en considération les aspects suivants:

- l'objectif de l'appréciation;
- les besoins des parties prenantes;
- toutes exigences légales, réglementaires et contractuelles;
- l'environnement et le scénario d'exploitation;
- l'importance de la décision (les conséquences si une mauvaise décision est prise, par exemple);
- tous les critères de décision définis et leur forme;
- le temps disponible avant de devoir prendre une décision;

- les informations disponibles ou qui peuvent être obtenues;
- la complexité de la situation;
- l'expertise disponible ou qui peut être obtenue.

Les caractéristiques des techniques permettant de satisfaire à ces exigences figurent dans le Tableau A.1. Le Tableau A.2 donne une liste des techniques, classées en fonction de ces caractéristiques.

Au fur et à mesure de l'augmentation du degré d'incertitude, de complexité et d'ambiguïté, la nécessité de consulter un groupe plus large de parties prenantes augmente, ce qui a des implications pour la combinaison des techniques choisies.

NOTE L'IEC TR 63039:2016 [50], par exemple, indique comment utiliser, de manière complémentaire, les techniques d'analyse par arbre d'événement (AAE), d'analyse par arbre de panne (AAP) et de Markov, de sorte que leur utilisation combinée soit un moyen efficace d'analyser le risque de systèmes complexes.

Les mêmes techniques décrites dans le présent document peuvent être appliquées lors des étapes du processus de management du risque de l'ISO 31000 en complément du cadre de leur utilisation dans l'appréciation du risque. L'application des techniques du processus de management du risque est représentée à la Figure A.1. Le Tableau A.3 représente leur application spécifique au cadre de l'appréciation.

L'Annexe B contient un aperçu général de chaque technique, de son utilisation, de ses entrées et sorties, de ses forces et limitations et, selon le cas, une référence indiquant où des détails supplémentaires peuvent être obtenus. Elle classe les techniques en fonction de leur application principale dans l'appréciation du risque, à savoir:

- obtenir les points de vue des parties prenantes et des experts (Article B.1);
- identifier le risque (Article B.2);
- déterminer les sources, les causes et les facteurs de risque (Article B.3);
- analyser les moyens de maîtrise existants (Article B.4);
- comprendre les conséquences et la vraisemblance (Article B.5);
- analyser les dépendances et les interactions (Article B.6);
- fournir des mesures du risque (Article B.7);
- évaluer l'importance d'un risque (Article B.8);
- faire un choix parmi des options (Article B.9);
- enregistrer et consigner (Article B.10).

Au sein de chaque groupe, les techniques sont classées par ordre alphabétique, sans tenir compte de leur importance.

La majorité des techniques décrites dans l'Annexe B prennent pour hypothèse que les risques ou les sources de risques peuvent être identifiés. Il existe également des techniques pouvant être utilisées pour apprécier indirectement le risque résiduel en tenant compte des moyens de maîtrise et des exigences en place (voir par exemple l'IEC 61508 [36]).

Même si le présent document traite de ces techniques et en donne des exemples, les techniques décrites ne sont pas exhaustives et aucune recommandation n'est formulée en ce qui concerne l'efficacité d'une technique précise, quelles que soient les circonstances. Il convient de veiller à choisir une technique en fonction de sa pertinence, de sa fiabilité et de son efficacité dans les circonstances données.

Annexe A (informative)

Catégorisation des techniques

A.1 Introduction à la catégorisation des techniques

Le Tableau A.1 décrit les caractéristiques des techniques qui peuvent être utilisées pour choisir la ou les techniques à utiliser.

Tableau A.1 – Caractéristiques des techniques

Caractéristique	Description	Détails (indicateurs des fonctions, etc.)
Application	Utilisation de la technique dans l'appréciation du risque (voir les titres des Articles B.1 à B.10)	Faire émerger des points de vue, identifier, analyser les causes, analyser les moyens de maîtrise, etc.
Domaine d'application	S'applique aux risques au niveau de l'organisation, du département ou du projet, ou au niveau des processus ou équipements individuels	organisation (org.) projet/département (dép.) équipements/processus (équip./proc.)
Horizon temporel	Etudie les risques à court, moyen ou long terme, ou s'applique à n'importe quel horizon temporel	Court, moyen, long, tout horizon temporel
Niveau de décision	S'applique aux risques au niveau stratégique, tactique ou opérationnel	Stratégique (1), tactique (2), opérationnel (3)
Niveau des informations/données de départ nécessaires	Niveau des informations ou données de départ nécessaires	Elevé, moyen, faible
Expertise des spécialistes	Niveau d'expertise exigé pour une utilisation correcte	faible: expertise intuitive ou formation d'un ou deux jours modérée: formation de plus de deux jours élevée: exige une formation poussée ou l'expertise d'un spécialiste
Qualitative – quantitative	Définit la méthode utilisée: qualitative, semi-quantitative ou quantitative	quantitative (quant.) qualitative (qual.) semi-quantitative (semi-quant.) les deux utilisations sont possibles (l'une ou l'autre)
Effort à appliquer	Durée et coût nécessaires pour appliquer la technique	élevé, moyen, faible

A.2 Application de la catégorisation des techniques

Le Tableau A.2 répertorie un ensemble de techniques classées selon ces caractéristiques. Les techniques décrites représentent des modes structurés d'observation du problème en cours ayant été jugés utiles dans des contextes particuliers. Cette liste n'est pas censée être complète, mais elle décrit un ensemble de techniques utilisées couramment dans différents secteurs. Pour simplifier la lecture, ces techniques sont classées par ordre alphabétique, sans priorité.

Chaque technique est décrite en détail à l'Annexe B, telle qu'elle est référencée dans la colonne 1 du Tableau A.2.

Tableau A.2 – Techniques et caractéristiques indicatives

Paragraphe	Technique	Description	Application	Domaine d'application	Horizon temporel	Niveau de décision	Niveau des informations/données de départ nécessaires	Expertise des spécialistes	Qual./quant./semi-quant.	Effort à appliquer
B.8.2	ALARP/SFAIRP	Critères de détermination de l'importance du risque et moyens d'évaluation de la tolérabilité du risque.	évaluer le risque	1	tous	1/2	élevé	élevée	qual./quant.	élevé
B.5.2	Analyse bayésienne	Méthode permettant d'établir des inférences relatives aux paramètres des modèles à l'aide du théorème de Bayes, qui permet d'intégrer des données empiriques à des avis préalables relatifs aux probabilités.	analyser la vraisemblance	tous	tous	tous	moyen	élevée	quant.	moyen
B.5.3	Réseaux bayésiens/diagrammes d'influence	Modèle graphique de variables et de leurs relations de cause à effet exprimées à l'aide de probabilités. Les réseaux bayésiens contiennent des variables représentant des incertitudes. Il existe des versions étendues, également appelées diagrammes d'influence, qui contiennent des variables représentant les incertitudes, les conséquences et les actions.	identifier le risque estimer le risque choisir entre plusieurs options	tous	tous	tous	moyen	élevée	quant.	moyen/ élevé
B.4.2	Analyse "nœud papillon"	Moyen schématique permettant de décrire un cheminement, des sources du risque à ses résultats, et de revoir les moyens de maîtrise.	analyser le risque analyser les moyens de maîtrise décrire le risque	2/3	court/moyen	tous	faible	faible/modérée	qual./semi-quant.	faible
B.1.2	"Brainstorming"	Technique utilisée lors des ateliers pour stimuler l'imagination.	faire émerger des points de vue	tous	tous	tous	aucune	faible/modérée	qual.	faible

Paragraphe	Technique	Description	Application	Domaine d'application	Horizon temporel	Niveau de décision	Niveau des informations/données de départ nécessaires	Expertise des spécialistes	Qual./quant./semi-quant.	Effort à appliquer
B.5.4	Analyse d'impact sur l'activité	Le processus d'AIA analyse les conséquences d'un incident perturbateur sur les modalités définissant les priorités en matière de récupération des produits et services d'une organisation et, par conséquent, les priorités des activités et ressources permettant de générer ces produits et services.	analyser les conség. analyser les moyens de maîtrise	1	court/moyen	2	moyen	faible	quant./qual.	moyen
B.6.1	Cartographie causale	Diagramme de réseau représentant les événements, les causes et les effets, ainsi que les relations entre ceux-ci.	analyser les causes	2/3	tous	2/3	moyen	modérée	qual.	moyen
B.5.5	Analyse causes-conséquences	Combinaison de l'analyse par arbre de panne et par arbre d'événement permettant d'inclure des actions différées. Les causes et les conséquences d'un événement initiateur sont prises en compte.	analyser les causes et les conség.	2/3	tous	2/3	moyen/élevé	modérée/élevée	quant.	moyen/élevé
B.2.2	Classifications des listes de contrôle, taxonomies	Création de listes basées sur l'expérience ou sur des concepts et modèles pouvant être utilisés pour identifier les risques et les moyens de maîtrise.	identifier les risques et les moyens de maîtrise	2/3	tous	tous	élevé (développement) faible (utilisation)	faible/modérée	qual.	faible/moyen
B.3.2	Approche cindynique	Prise en compte des objectifs, des valeurs, des règles, des données et des modèles des parties prenantes et identification des incohérences, des ambiguïtés, des omissions et des lacunes. Ces éléments constituent les sources systémiques et les facteurs de risque.	identifier les facteurs de risque	1/2	court ou moyen	1	faible	modérée	qual.	élevée
B.7.3	Valeur en risque conditionnelle	Egalement appelée "expected shortfall" (ES), cette valeur mesure la perte attendue d'un portefeuille financier dans les a % des scénarios les plus défavorables.	mesure du risque	tous	court/moyen	3	élevé	élevée	quant.	moyen

Paragraphe	Technique	Description	Application	Domaine d'application	Horizon temporel	Niveau de décision	Niveau des informations/données de départ nécessaires	Expertise des spécialistes	Qual./quant./semi-quant.	Effort à appliquer
B.10.3	Matrice conséquence/vraisemblance	Comparaison des risques individuels en choisissant une paire conséquence/vraisemblance et en l'affichant dans une matrice comportant un axe des conséquences et un axe de vraisemblance.	établir un rapport des risques évaluer	tous	tous	tous	moyen	faible (utilisation), moyen (développement)	qual./semi-quant./quant.	faible
B.9.2	Analyse coût/bénéfice	Analyse utilisant l'unité monétaire pour évaluer les conséquences positives et négatives, récupérables et irrécupérables des différentes options.	comparer les options	tous	court/moyen	tous	moyen/élevé	modérée/élevée	quant.	moyen/élevé
B.6.2	Analyse d'impacts croisés	Évaluation des variations de la probabilité qu'une série donnée d'événements se produise suite à la survenue réelle de l'un de ces événements.	analyser la vraisemblance et la cause	tous	court/moyen	tous	faible à élevé	modérée/élevée	quant.	moyen/élevé
B.9.3	Analyse par arbre de décision	Analyse utilisant une représentation sous forme d'arbre ou un modèle de décisions et leurs conséquences possibles. Les résultats sont généralement exprimés en termes monétaires ou en termes d'utilité. Autre représentation possible: le diagramme d'influence (voir B.5.3).	comparer les options	tous	tous	2	faible/moyen	modérée	quant.	moyen
B.1.3	Technique Delphi	Collecte d'avis par l'intermédiaire de questionnaires séquentiels. Les personnes interrogées répondent individuellement, mais reçoivent des commentaires sur les réponses des autres personnes après chaque série de questions.	faire émerger des points de vue	tous	tous	tous	aucune	modérée	qual.	moyen
B.5.6	Analyse par arbre d'événement (AAE)	Modélisation des résultats possibles d'un événement initiateur donné et du statut des moyens de maîtrise de manière à analyser la fréquence ou la probabilité des différents résultats possibles.	analyser les conséq. et les moyens de maîtrise	2/3	tous	tous	faible/moyen	modérée	qual./quant.	moyen

Paragraphe	Technique	Description	Application	Domaine d'application	Horizon temporel	Niveau de décision	Niveau des informations/données de départ nécessaires	Expertise des spécialistes	Qual./quant./semi-quant.	Effort à appliquer
B.5.7	Analyse par arbre de panne (AAP)	Analyse des causes d'un événement précis à l'aide de la logique booléenne pour décrire une combinaison de pannes. Variations possibles: arbre de réussite dans lequel l'événement de tête est souhaité ou arbre des causes utilisé pour étudier les événements passés.	analyser la vraisemblance analyser les causes	2/3	moyen	2/3	élevé pour l'analyse quantitative	dépend de la complexité	qual./quant.	moyen/élevé
B.2.3	Analyse des modes de défaillance et de leurs effets (et de leur criticité) AMDE(C)	Etude des modes de défaillance possibles de chaque composant d'un système et des causes et effets de ces défaillances. L'AMDE peut être suivie d'une analyse de criticité qui définit l'importance de chaque mode de défaillance (AMDEC).	identifier les risques	2/3	tous	2/3	selon l'application	modérée	qual./semi-quant./quant.	faible/élevé
B.8.3	Diagrammes fréquence/nombre (F/N)	Cas particulier de graphique de conséquence/vraisemblance quantitative appliqué à la prise en compte de la tolérabilité du risque auquel sont exposées les vies humaines.	évaluer le risque	1	tous	tous	élevé	élevée	quant.	élevé
B.9.4	Théorie des jeux	Etude de la prise de décision stratégique pour modéliser l'impact des décisions des différents joueurs impliqués dans le jeu. L'établissement de tarifs basés sur les risques peut être un exemple de domaine d'application.	choisir entre plusieurs options	1	moyen	1/2	élevé	élevée	quant.	moyen/élevé
B.4.3	Analyse des dangers – points critiques pour leur maîtrise (HACCP)	Analyse de la réduction du risque pouvant être obtenue par différents niveaux de protection.	analyser les moyens de maîtrise et de surveillance	2/3	court/moyen	2/3	moyen	modérée	qual.	moyen

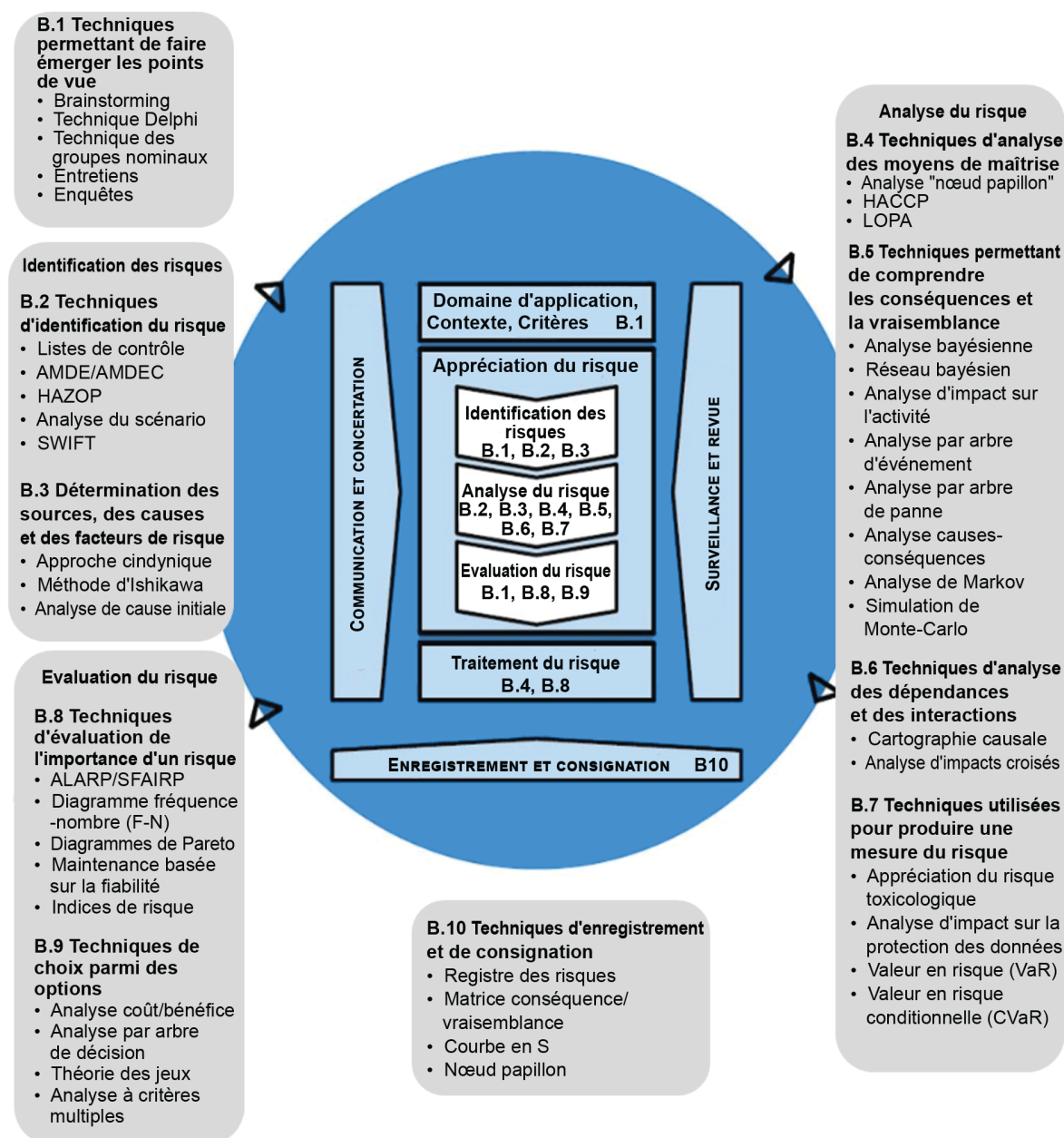
Paragraphe	Technique	Description	Application	Domaine d'application	Horizon temporel	Niveau de décision	Niveau des informations/données de départ nécessaires	Expertise des spécialistes	Qual./quant./semi-quant.	Effort à appliquer
B.2.4	Etudes de danger et d'exploitabilité (HAZOP)	Examen structuré et systématique d'un processus ou d'un fonctionnement planifié ou existant permettant d'identifier et d'évaluer les problèmes pouvant représenter un risque pour le personnel ou les équipements, ou pouvant empêcher un fonctionnement efficace.	identifier et analyser les risques	3	moyen/long	2/3	moyen	animateur: élevée, participants: modérée	qual.	moyen/élevé
B.5.8	Analyse de fiabilité humaine (AFH)	Ensemble de techniques permettant d'identifier le potentiel d'erreur humaine et d'estimer la vraisemblance d'une défaillance.	analyser les risques et les sources de risques	2/3	tous	2/3	moyen	élevée	qual./quant.	moyen à élevé
B.1.5	Entretiens	Conversations structurées ou semi-structurées en tête à tête permettant de faire émerger des points de vue.	faire émerger des points de vue	tous	tous	tous	aucune	modérée	qual.	élevé
B.3.3	Analyse d'Ishikawa (diagramme en arêtes de poisson)	Identification des facteurs contributifs à l'origine d'un résultat défini (souhaité ou non souhaité). Les facteurs contributifs sont généralement divisés en catégories prédéfinies et affichés sous la forme d'une arborescence ou d'un diagramme d'Ishikawa.	analyser les sources de risques	tous	tous	tous	faible	faible/modérée	qual.	faible
B.4.4	Méthode LOPA	Analyse de la réduction du risque pouvant être obtenue par différents niveaux de protection.	analyser les moyens de maîtrise	3	tous	2/3	moyen	modérée/élevée	qual./quant.	moyen/élevé
B.5.9	Analyse de Markov	Calcul de la probabilité qu'un système pouvant être associé à différents états se trouve dans un état donné à un instant <i>t</i> dans le futur.	analyser la vraisemblance	3	tous	2/3	moyen/élevé	élevée	quant.	moyen
B.5.10	Analyse de Monte-Carlo	Calcul de la probabilité des résultats en procédant à plusieurs simulations à l'aide de variables aléatoires.	analyser la vraisemblance	tous	tous	tous	moyen	élevée	quant.	moyen/élevé

Paragraphe	Technique	Description	Application	Domaine d'application	Horizon temporel	Niveau de décision	Niveau des informations/données de départ nécessaires	Expertise des spécialistes	Qual./quant./semi-quant.	Effort à appliquer
B.9.5	Analyse à critères multiples (ACM)	Comparaison des options de manière à rendre les compromis explicites. Propose une autre analyse que l'analyse coût/bénéfice pour laquelle il n'est pas nécessaire d'allouer une valeur monétaire à toutes les entrées.	choisir entre plusieurs options	tous	tous	tous	faible	modérée	qual.	faible/moyen
B.1.4	Technique des groupes nominaux	Technique permettant de faire émerger des points de vue dans un groupe dont les membres s'expriment d'abord de manière individuelle, sans interaction, puis discutent en groupe de leurs idées.	faire émerger des points de vue	tous	tous	tous	aucune	faible	qual.	moyen
B.8.4	Diagrammes de Pareto	Selon le principe de Pareto (loi des 80/20), pour de nombreux événements, environ 80 % des effets sont produits par 20 % des causes.	définir des priorités	tous	tous	tous	moyen	modérée	semi-quant./quant.	faible
B.5.11	Analyse d'impact sur la vie privée/appréciation des impacts sur la protection des données (PIA/DPIA)	Permet d'analyser la manière dont les incidents et les événements pourraient avoir un impact sur la vie privée d'une personne, et d'identifier et de quantifier les aptitudes nécessaires à leur gestion.	analyser les sources de risques analyse conséq.	tous	tous	1/2	moyen	modérée/élevée	qual.	moyen
B.8.5	Maintenance basée sur la fiabilité (MBF)	Evaluation basée sur les risques utilisée pour identifier les tâches de maintenance appropriées pour un système et ses composants.	évaluer le risque choisir des moyens de maîtrise	2/3	moyen	2/3	moyen	élevée pour l'animateur, modérée à utiliser	qual./semi-quant./quant.	moyen/élevé
B.8.6	Indices de risque	Estimation de l'importance des risques en fonction de classements appliqués à des facteurs censés influencer sur l'ampleur du risque.	comparer les risques	tous	tous	tous	moyen	faible (utilisation), moyen (développement)	semi-quant.	faible
B.10.2	Registres des risques	Support permettant d'enregistrer les informations relatives aux risques et d'effectuer un suivi des actions.	enregistrement et consignation des risques surveillance et revue	tous	tous	tous	faible/moyen	faible/modérée	qual.	moyen

Paragraphe	Technique	Description	Application	Domaine d'application	Horizon temporel	Niveau de décision	Niveau des informations/données de départ nécessaires	Expertise des spécialistes	Qual./quant./semi-quant.	Effort à appliquer
B.10.4	Courbes en S	Représentation des relations entre les conséquences et leur vraisemblance sous la forme d'une fonction de distribution cumulative (courbe en S).	afficher les risques évaluer le risque	tous	tous	2/3	moyen/élevé	modérée/élevée	quant./semi-quant.	moyen
B.2.5	Analyse du scénario	Permet d'imaginer ou de modéliser les futurs scénarios possibles, ou de les extrapoler à partir du présent. Le risque est alors pris en compte pour chacun de ces scénarios.	identifier les risques, analyse des conséq.	tous	moyen ou long	tous	faible/moyen	modérée	qual.	faible/moyen
B.1.6	Enquêtes	Questionnaires papier ou électronique permettant de faire émerger des points de vue.	faire émerger des points de vue	tous	moyen/long	2/3	faible	modérée	qual.	élevé
B.2.6	Méthode SWIFT ("Que se passerait-il si?")	Forme simplifiée de la méthode HAZOP basée sur des questions du type "Que se passerait-il si" permettant d'identifier les écarts par rapport à la situation attendue.	identifier le risque	1/2	moyen/long	1/2	moyen	faible/modérée	qual.	faible/moyen
B.7.1	Appréciation du risque toxicologique	Procédure permettant de mesurer le risque auquel sont exposés les êtres humains et les systèmes écologiques en présence de produits chimiques.	mesure du risque	3	moyen/long	2/3	élevé	élevée	quant.	élevé
B.7.2	Valeur en risque (VaR)	Mesure financière du risque utilisant une probabilité supposée de répartition des pertes dans un marché stable pour calculer la valeur d'une perte pouvant survenir selon une probabilité donnée au cours d'une période définie.	mesure du risque	tous	court/moyen	3	élevé	élevée	quant.	moyen

A.3 Utilisation des techniques au cours du processus ISO 31000

Le Tableau A.3 indique dans quelle mesure chaque technique est applicable aux différents stades d'appréciation du risque, à savoir l'identification du risque, l'analyse du risque et l'évaluation du risque. Certaines des techniques sont également utilisées dans d'autres étapes du processus. Ceci est représenté à la Figure A.1.



IEC

Figure A.1 – Application des techniques au processus de management du risque ISO 31000 [3]

NOTE La Figure A.1 est destinée à fournir une présentation générale et ne constitue pas une liste exhaustive de toutes les techniques pouvant être utilisées à chaque étape.

Tableau A.3 – Applicabilité des techniques au processus ISO 31000

Outils et techniques	Processus d'évaluation des risques					Paragraphe
	Identification des risques	Analyse du risque			Evaluation du risque	
		Conséquence	Vraisemblance	Niveau de risque		
ALARP, ALARA et SFAIRP	NA	NA	NA	NA	FA	B.8.2
Analyse bayésienne	NA	NA	FA	NA	NA	B.5.2
Réseaux bayésiens	NA	NA	FA	NA	FA	B.5.3
Analyse "nœud papillon"	A	FA	A	A	A	B.4.2
"Brainstorming"	FA	A	NA	NA	NA	B.1.2
Analyse d'impact sur l'activité	A	FA	NA	NA	NA	B.5.4
Cartographie causale	A	A	NA	NA	NA	B.6.1
Analyse causes/conséquences	A	FA	FA	A	A	B.5.5
Listes de contrôle, classifications et taxonomies	FA	NA	NA	NA	NA	B.2.2
Approche cindynique	FA	NA	NA	NA	NA	B.3.2
Matrice conséquence/vraisemblance	NA	A	A	FA	A	B.10.3
Analyse coût/bénéfice	NA	FA	NA	NA	FA	B.9.2
Analyse d'impacts croisés	NA	NA	FA	NA	NA	B.6.2
Analyse par arbre de décision	NA	FA	FA	A	A	B.9.3
Technique Delphi	FA	NA	NA	NA	NA	B.1.3
Analyse par arbre d'événement	NA	FA	A	A	A	B.5.6
Analyse des modes de défaillances et de leurs effets	FA	FA	NA	NA	NA	B.2.3
Analyse des modes de défaillance, de leurs effets et de leur criticité	FA	FA	FA	FA	FA	B.2.3
Analyse par arbre de panne	A	NA	FA	A	A	B.5.7
Diagrammes F/N	A	FA	FA	A	FA	B.8.3
Théorie des jeux	A	FA	NA	NA	FA	B.9.4
Etudes de danger et d'exploitabilité (HAZOP)	FA	A	NA	NA	NA	B.2.4
Analyse des dangers – points critiques pour leur maîtrise (HACCP)	FA	FA	NA	NA	FA	B.4.3
Analyse de fiabilité humaine	FA	FA	FA	FA	A	B.5.8
Ishikawa (en arêtes de poisson)	FA	A	NA	NA	NA	B.3.3
Méthode LOPA	A	FA	A	A	NA	B.4.4
Analyse de Markov	A	A	FA	NA	NA	B.5.9
Simulation de Monte-Carlo	NA	A	A	A	FA	B.5.10
Analyse à critères multiples (ACM)	A	NA	NA	NA	FA	B.9.5
Technique des groupes nominaux	FA	A	A	NA	NA	B.1.4
Diagrammes de Pareto	NA	A	A	A	FA	B.8.4
(PIA/DPIA) Analyse d'impact sur la vie privée / Analyse d'impact sur la protection des données	A	FA	A	A	FA	B.5.11

Annexe B (informative)

Description des techniques

B.1 Techniques permettant de faire émerger les points de vue des parties prenantes et des experts

B.1.1 Généralités

Certaines des techniques décrites dans les Articles B.2 à B.7 impliquent une intervention des différents experts et parties prenantes. Ce mode de fonctionnement permet de bénéficier d'une large expertise et de favoriser l'implication des parties prenantes. Les points de vue des parties prenantes et des experts peuvent être recueillis sur une base individuelle (par un entretien ou une enquête, par exemple) ou à l'aide de techniques de groupe telles que le "brainstorming", les groupes nominaux ou la technique Delphi. L'expression "points de vue" peut comprendre la divulgation d'informations, l'expression d'opinions ou l'émergence d'idées novatrices. L'Article B.1 décrit quelques techniques pouvant être utilisées pour faire émerger des informations ou créer un consensus.

Dans certaines situations, les différentes parties prenantes ont une expertise spécifique ou sont associées à un rôle précis: les divergences d'opinions sont alors peu nombreuses. Toutefois, il arrive que des points de vue divergents soient à prévoir et que les structures hiérarchiques ou d'autres facteurs influent sur les interactions des différentes personnes. Ces facteurs détermineront le choix de la méthode utilisée. Le nombre de parties prenantes à consulter, les contraintes de temps et les aspects pratiques liés au regroupement simultané de toutes les personnes concernées influenceront également sur le choix de la méthode.

Lorsqu'une méthode de groupe en face à face est utilisée, il est important de désigner un animateur qualifié et expérimenté pour obtenir de bons résultats. Le rôle de l'animateur ou du coordinateur est le suivant:

- organiser l'équipe;
- obtenir et distribuer les informations et données utiles préalablement à la réunion/séance de travail collaboratif;
- préparer le cadre et les modalités de la réunion/séance de travail collaboratif;
- stimuler la créativité afin d'améliorer la compréhension et de générer des idées;
- garantir l'exactitude et la neutralité des résultats.

Les listes de contrôle dérivées des classifications et des taxonomies peuvent être utilisées dans le cadre du processus (voir B.2.2).

Toutes les techniques de collecte d'informations qui s'appuient sur les perceptions et les opinions des personnes risquent de ne pas être complètement fiables et d'être entachées de différents partis pris tels que le biais de disponibilité (tendance à surestimer la vraisemblance d'un événement qui vient de survenir), l'illusion des séries (tendance à surestimer l'importance des petites séries dans un échantillon de grande taille) ou l'effet de mode (tendance à faire ou à croire ce que font ou croient les autres personnes).

L'EN 12973 [4] contient des recommandations sur l'analyse fonctionnelle qui peuvent être utilisées pour réduire ces partis pris et orienter la créativité vers les aspects ayant l'impact le plus important.

Il convient de consigner dans un rapport les informations à partir desquelles ont été formulés les avis et les hypothèses éventuelles.

B.1.2 "Brainstorming"

B.1.2.1 Vue d'ensemble

Le "brainstorming" est un processus utilisé pour stimuler et encourager un groupe de personnes à développer des idées relatives à un ou plusieurs sujets de quelque nature que ce soit. Le terme "brainstorming" est souvent utilisé très librement pour signifier tout type de discussion en groupe, mais un "brainstorming" efficace exige un effort délibéré afin que les pensées des autres personnes du groupe soient utilisées pour stimuler la créativité de chaque participant. Toute analyse ou critique des idées est formulée en dehors du "brainstorming".

Cette technique donne des résultats optimaux en présence d'un animateur expert pouvant stimuler les participants sans brider la pensée. L'animateur encourage le groupe à traiter de tous les domaines concernés et s'assure que les idées issues de ce processus sont conservées afin d'être analysées par la suite.

Le "brainstorming" peut être structuré ou non structuré. Lorsque le "brainstorming" est structuré, l'animateur scinde l'objet de la discussion en plusieurs parties et utilise des questions préparées pour susciter des idées sur un nouveau sujet lorsqu'un thème est épuisé. Le "brainstorming" non structuré est souvent moins formel. Dans les deux cas, l'animateur avance une série d'éléments de réflexion et tous les participants sont invités à émettre des idées. Le rythme de la séance est soutenu afin de permettre l'émergence de pensées latérales. L'animateur peut orienter différemment la discussion ou utiliser un autre outil de pensée créative lorsqu'une piste de réflexion est épuisée ou que la discussion s'écarte trop du sujet. L'objectif est de rassembler autant d'idées diverses que possible en vue d'une analyse ultérieure.

Il a été prouvé qu'en pratique, un groupe génère moins d'idées que ses membres lorsqu'ils travaillent individuellement. Par exemple,

- au sein d'un groupe, les idées ont tendance à converger plutôt qu'à se diversifier;
- le délai d'attente de prise de la parole a tendance à bloquer les idées;
- les individus ont tendance à fournir un effort mental moins important lorsqu'ils sont en groupe.

Ces tendances peuvent être réduites en:

- donnant aux individus concernés l'occasion de travailler seul une partie du temps;
- diversifiant les équipes et en modifiant la composition de celles-ci;
- utilisant d'autres techniques, telles que la technique des groupes nominaux (B.1.4) ou le "brainstorming" électronique. Celles-ci encouragent la participation individuelle et peuvent être utilisées de manière anonyme, ce qui permet d'éviter les questions d'ordre personnel, politique et culturel.

B.1.2.2 Utilisation

Le "brainstorming" peut être appliqué à n'importe quel niveau d'une organisation pour identifier les incertitudes, les modes de réussite ou de défaillance, les causes, les conséquences, les critères de décision ou les options de traitement. Une utilisation quantitative du "brainstorming" est possible, mais uniquement dans sa forme structurée afin de garantir la prise en compte et la gestion des partis pris, notamment lorsque toutes les parties prenantes sont impliquées.

Cette technique qui stimule la créativité est donc très utile lors de la création de conceptions, produits et processus novateurs.

B.1.2.3 Entrées

Le "brainstorming" ayant pour objectif de faire émerger les points de vue des participants, il nécessite moins de données ou informations externes que les autres méthodes. Les participants à l'exercice ont besoin de disposer de l'expertise et de l'expérience nécessaires et d'être en mesure d'émettre divers points de vue relatifs au problème étudié. Pour que le "brainstorming" soit productif, un animateur qualifié est nécessaire.

B.1.2.4 Résultats

Le résultat du "brainstorming" est une liste de toutes les idées générées au cours de la séance et des pensées formulées lors de leur présentation.

B.1.2.5 Avantages et limites

Les avantages du "brainstorming" incluent ce qui suit.

- Il stimule l'imagination et la créativité, permettant ainsi d'identifier de nouveaux risques et des solutions originales.
- Il est utile lorsque les données de départ sont peu nombreuses ou inexistantes, ou lorsque l'utilisation de nouvelles technologies ou de solutions originales est exigée.
- Il implique des parties prenantes clés et facilite donc la communication et l'engagement.
- Il est relativement rapide et facile à mettre en place.

Les limites incluent ce qui suit.

- Il est difficile de démontrer que le processus est exhaustif.
- Les groupes ont tendance à générer moins d'idées que des individus travaillant seuls.
- Lorsque la dynamique de groupe est variable, il peut arriver que les personnes ayant de bonnes idées ne s'expriment pas, alors que d'autres monopolisent la discussion. Un animateur efficace peut éviter ces travers.
- Encourager la créativité et les idées nouvelles peut signifier que la conversation ne reste pas focalisée sur les questions à l'étude et ceci prend le temps de la réunion.

B.1.2.6 Documents de référence

- [5] PROCTOR, A. (2009). *Creative problem solving for managers*
- [6] GOLDENBERG, Olga, WILEY, Jennifer. *Quality, conformity, and conflict: Questioning the assumptions of Osborn's brainstorming technique*

B.1.3 Technique Delphi

B.1.3.1 Vue d'ensemble

La technique Delphi permet de créer un consensus sur les opinions d'un groupe d'experts. Cette méthode vise à collecter et rassembler des avis sur un sujet donné en s'appuyant sur une série de questionnaires séquentiels. L'une des fonctions essentielles de la technique Delphi consiste à permettre à des experts d'exprimer leur avis de manière individuelle, indépendante et anonyme, tout en ayant accès aux avis de leurs homologues au fur et à mesure de l'avancement du processus.

La ou les questions sont soumises séparément à chacun des membres du groupe d'experts. Les informations provenant des premières réponses sont analysées et combinées, puis retransmises aux différents participants, qui peuvent alors reconsidérer leur réponse initiale. Les membres du groupe répondent, puis le processus est de nouveau enclenché tant qu'un consensus complet ou partiel n'a pas été obtenu. Si un membre du groupe ou une minorité de membres maintiennent leur réponse, cela signifie peut-être qu'ils disposent d'informations importantes ou que leur point de vue est essentiel.

B.1.3.2 Utilisation

La technique Delphi permet de résoudre des problèmes complexes pour lesquels il existe une incertitude rendant nécessaire l'avis d'experts. Elle peut être utilisée pour établir des prévisions et des politiques, arriver à un consensus ou aplanir des divergences d'opinions entre différents experts. Elle peut être utilisée pour identifier les risques (avec des résultats positifs et négatifs), les menaces et les opportunités, mais également pour créer un consensus sur la vraisemblance d'événements futurs et sur leurs conséquences. Elle est généralement utilisée au niveau stratégique ou tactique. Initialement destinée à établir des prévisions à long terme, elle peut en réalité être appliquée à tous les types de prévisions.

B.1.3.3 Entrées

Cette méthode repose sur les connaissances et la coopération continue des participants pendant une période variable pouvant s'étendre sur plusieurs jours, semaines, mois ou années.

Le nombre de participants peut varier entre quelques individus et des centaines de personnes. Les questionnaires peuvent être au format papier ou être distribués et renvoyés à l'aide d'outils de communication électronique (courrier électronique ou Internet). L'utilisation de systèmes technologiques permet d'apporter souplesse et la précision à la compilation des informations à chaque cycle.

B.1.3.4 Résultats

Consensus sur les questions à l'étude.

B.1.3.5 Avantages et limites

Les avantages incluent ce qui suit.

- Compte tenu de leur caractère anonyme, les avis impopulaires sont plus susceptibles d'être exprimés et les partis pris liés à la hiérarchie s'en trouvent amoindris.
- Tous les points de vue sont pondérés de manière égale (il s'agit d'éviter tous les problèmes liés aux personnalités dominatrices).
- Cette technique permet d'obtenir la propriété des résultats.
- Il n'est pas nécessaire que les personnes soient rassemblées en même temps au même endroit.
- Les participants ont le temps de suffisamment réfléchir à leurs réponses aux questions.
- Le processus a tendance à faire que les experts consacrent pleinement leur attention à la tâche qui leur incombe.

Les limites incluent ce qui suit.

- Cela demande beaucoup de travail et de temps.
- Il est nécessaire que les participants soient capables de s'exprimer correctement par écrit.

B.1.3.6 Document de référence

- [7] ROWE, G. WRIGHT, G. The Delphi technique: Past, present, and future prospects. *Technological forecasting and social change* 2011, 78, Special Delphi Issue

B.1.4 Technique des groupes nominaux

B.1.4.1 Vue d'ensemble

Comme le "brainstorming", la technique des groupes nominaux a pour objectif de collecter des idées. Les points de vue sont recueillis individuellement, sans interaction entre les membres du groupe, puis ils font l'objet d'une discussion au niveau du groupe.

Le processus est le suivant.

- L'animateur soumet à chaque membre du groupe les questions auxquelles ce dernier devra répondre.
- Chaque participant écrit sa réponse seul et en silence.
- Chaque membre du groupe présente alors ses idées, mais la discussion n'est pas engagée à ce stade. Si la dynamique du groupe est telle que certaines voix ont plus de poids que d'autres, certaines idées peuvent être communiquées à l'animateur de manière anonyme. Les participants peuvent alors demander à obtenir des informations complémentaires.
- Les idées font alors l'objet d'une discussion au sein du groupe, qui en établit la liste d'un commun accord.
- Les membres du groupe votent secrètement pour une idée ou une autre et une décision de groupe est prise en fonction de ces votes.

B.1.4.2 Utilisation

La technique des groupes nominaux peut être utilisée à la place du "brainstorming". Elle est également utile pour affecter des priorités aux idées au sein d'un groupe.

B.1.4.3 Entrées

Les idées et l'expérience des participants.

B.1.4.4 Résultats

Idées, solutions ou décisions, selon les besoins définis.

B.1.4.5 Avantages et limites

Les avantages de la technique des groupes nominaux incluent ce qui suit.

- Elle permet d'obtenir une vision plus équilibrée que le "brainstorming" lorsque certains membres d'un groupe ont plus de facilité à s'exprimer à l'oral que d'autres.
- Elle a tendance à générer une meilleure participation si une partie ou l'ensemble des membres du groupe sont nouveaux dans l'équipe, si la question suscite la controverse ou s'il existe un déséquilibre des rapports de force ou un conflit au sein de l'équipe.
- Il a été prouvé qu'elle permet de générer davantage d'idées que le "brainstorming".
- Elle réduit la pression à se conformer au groupe.
- Elle peut créer un consensus à une relativement brève échéance.

Les limites incluent ce qui suit.

- La fertilisation croisée des idées peut être limitée.
- Les mêmes idées peuvent être exprimées de nombreuses manières légèrement différentes, ce qui complique d'autant leur consolidation.

B.1.4.6 Document de référence

- [8] MCDONALD, D. BAMMER, G. and DEANE, P. *Research Integration Using Dialogue Methods*

NOTE Cette étude donne également des informations sur plusieurs autres méthodes, dont certaines sont aussi abordées dans le présent document.

B.1.5 Entretiens structurés ou semi-structurés

B.1.5.1 Vue d'ensemble

Lors d'un entretien structuré, un ensemble de questions préparées est posé aux personnes interrogées. L'entretien semi-structuré est similaire, mais offre plus de liberté à la conversation pour explorer les questions soulevées. Il permet, en outre, d'explorer les domaines que la personne interrogée pourrait souhaiter traiter.

Dans la mesure du possible, il convient que les questions soient ouvertes, simples et exprimées dans la langue de la personne interrogée, et qu'elles ne traitent que d'un seul point. Des questions complémentaires possibles pour obtenir des éclaircissements sont également préparées.

Afin de vérifier que les questions ne sont pas ambiguës, qu'elles seront correctement comprises et que les réponses seront en rapport avec les sujets abordés, il convient de poser ces questions au préalable à des personnes ayant un profil similaire à celui des personnes interrogées. Il convient de veiller à ne pas influencer la personne interrogée.

B.1.5.2 Utilisation

Les entretiens structurés et semi-structurés permettent de collecter des informations et des avis précis auprès des individus d'un groupe. Si nécessaire, les réponses peuvent rester confidentielles. Leur contenu est d'autant plus intéressant que leurs auteurs ne sont pas influencés par les opinions des autres membres du groupe.

Les entretiens de ce type sont utiles s'il est difficile de réunir tous les participants simultanément dans un même lieu, ou si une discussion libre en groupe n'est pas appropriée compte tenu de la situation ou des personnes impliquées. Un entretien peut également permettre de collecter des informations plus précises qu'une enquête ou un atelier. Les entretiens peuvent être utilisés à tous les niveaux d'une organisation.

B.1.5.3 Entrées

Une bonne compréhension des informations nécessaires et une série de questions préparées ayant déjà été posées à un groupe pilote sont les éléments préalables à tout entretien.

Il est nécessaire que les personnes chargées de concevoir l'entretien et celles qui posent les questions aient les qualifications nécessaires pour obtenir des réponses valides non biaisées par les partis pris des personnes posant les questions.

B.1.5.4 Résultats

Le terme "résultat" couvre les informations détaillées exigées.

B.1.5.5 Avantages et limites

Les avantages des entretiens structurés incluent ce qui suit.

- Ils permettent aux personnes interrogées de prendre le temps de réfléchir à une question.
- La communication en tête à tête peut permettre d'étudier les questions de manière plus approfondie qu'une approche en groupe.
- Les entretiens structurés permettent d'impliquer un plus grand nombre de parties prenantes qu'un groupe en face à face.

Les limites incluent ce qui suit.

- La conception, la réalisation et l'analyse des entretiens demandent beaucoup de temps.

- Leur conception et leur réalisation exigent une certaine expertise si les réponses ne doivent pas être biaisées par la personne qui pose les questions.
- Les partis pris dans les réponses sont tolérés, ils ne sont ni modérés, ni supprimés de la discussion de groupe.
- Les entretiens ne stimulent pas l'imagination (alors que tel est le cas avec les méthodes de groupe).
- Les entretiens semi-structurés génèrent une masse considérable d'informations exprimées avec les mots de la personne interrogée. Il peut être difficile de regrouper ces informations sans ambiguïté sous une forme appropriée à l'analyse.

B.1.5.6 Documents de référence

- [9] HARRELL, M.C. BRADLEY, M.A. 2009, *Data collection methods – A training Manual – Semi structured interviews and focus groups*
- [10] GILL, J. JOHNSON, P. 2010, *Research methods for managers*

B.1.6 Enquêtes

B.1.6.1 Vue d'ensemble

De manière générale, les enquêtes permettent d'impliquer davantage de personnes et de poser des questions plus précises que les entretiens. Le plus souvent, une enquête prendra la forme d'un questionnaire papier ou électronique. Les réponses aux questions sont généralement de type oui/non, ou prennent la forme de différents choix possibles dans une échelle de classement ou une série d'options. Une analyse statistique des résultats, qui est une caractéristique de ces méthodes, est ainsi possible. Une enquête peut comporter des questions appelant une réponse libre, mais il convient d'en limiter le nombre en raison des difficultés d'analyse.

B.1.6.2 Utilisation

Les enquêtes peuvent être utilisées dans toutes les situations où une vaste concertation des parties prenantes est utile, notamment lorsque l'objectif est de recueillir un nombre relativement restreint d'informations auprès d'un grand nombre de personnes.

B.1.6.3 Entrées

Des questions non ambiguës préalablement posées à d'autres personnes, et envoyées à un échantillon largement représentatif des personnes souhaitant participer. Il est nécessaire que le nombre de réponses soit suffisant pour garantir la validité statistique de l'enquête. (Les taux de retour sont souvent faibles, ce qui signifie qu'il est nécessaire d'envoyer de nombreux questionnaires.) Une certaine expertise est nécessaire pour élaborer un questionnaire dont les résultats seront utiles et pour procéder à l'analyse statistique des résultats.

B.1.6.4 Résultats

Le résultat est une analyse des points de vue d'une série d'individus, souvent présentée sous forme graphique.

B.1.6.5 Avantages et limites

Les avantages des enquêtes incluent ce qui suit.

- Elles peuvent impliquer un plus grand nombre de participants que les entretiens, ce qui permet de générer des informations plus intéressantes au sein d'un groupe.
- Les enquêtes ont un coût relativement faible, notamment en cas d'utilisation d'un logiciel en ligne capable d'effectuer une analyse statistique.
- Elles peuvent générer des informations statistiquement valides.

- Les résultats sont faciles à exprimer sous forme de tableaux et à comprendre: une sortie graphique est généralement possible.
- Des rapports relatifs aux enquêtes peuvent assez facilement être mis à la disposition des autres utilisateurs.

Les limites incluent ce qui suit.

- Le contenu des questions est limité par la nécessité de les exprimer simplement et sans ambiguïté.
- Il est généralement nécessaire d'obtenir des informations démographiques pour interpréter les résultats.
- Le nombre de questions d'un questionnaire est limité si l'objectif est de collecter un nombre suffisant de réponses.
- La personne qui pose les questions ne peut pas les expliquer: les participants à l'enquête peuvent donc leur attribuer un sens autre que celui qu'elles avaient initialement.
- Il est difficile de concevoir des questions qui n'amènent pas les participants à l'enquête à choisir une réponse en particulier.
- Les questionnaires tendent à surligner des hypothèses qui ne pourraient pas être valides.
- Il peut être difficile d'obtenir un taux de réponse satisfaisant et sans parti pris.

B.1.6.6 Documents de référence

[11] SAUNDERS, M. LEWIS, P. THORNHILL, A. 2016, *Research Methods for Business Students*

[12] UNIVERSITY OF KANSAS COMMUNITY TOOL BOX Section 13 *Conducting surveys*

B.2 Techniques d'identification du risque

B.2.1 Généralités

Les techniques d'identification des risques peuvent inclure:

- des méthodes reposant sur la preuve, telles que des revues bibliographiques et des analyses de données historiques;
- des méthodes empiriques, notamment des techniques d'essai et de modélisation permettant d'identifier ce qui pourrait se passer dans des circonstances particulières;
- des enquêtes de perception qui permettent de sonder les points de vue d'un grand nombre de personnes expérimentées;
- des techniques dans lesquelles le sujet à étudier est divisé en sous-éléments, qui sont traités les uns après les autres à l'aide de méthodes ayant recours à des questions du type "Que se passerait-il si";

EXAMPLES Les méthodes HAZOP (B.2.4), AMDE (B.2.3) et SWIFT (B.2.6).

- des techniques stimulant la créativité en matière de possibilités futures, telles que l'analyse de scénario (B.2.5);
- des listes de contrôle ou des taxonomies basées sur d'anciennes données ou des modèles théoriques (B.2.2).

Les techniques décrites à l'Article B.2 sont des exemples d'approches structurées permettant d'identifier les risques. Les techniques structurées sont généralement plus complètes que les techniques non structurées ou semi-structurées. Elles permettent de procéder plus facilement aux contrôles préalables lors de l'identification des risques.

L'utilisation de plusieurs techniques, y compris à la fois des méthodes descendantes et ascendantes, favorise une identification complète des risques. Des approches qui remettent en cause les résultats de l'identification des risques, telles que la constitution d'une "équipe rouge", peuvent également être utilisées pour vérifier qu'aucun risque pertinent n'a été négligé.

NOTE Une équipe rouge (*red teaming*) est une pratique qui consiste à visualiser un problème du point de vue d'un adversaire ou d'un concurrent. [13].

Les techniques décrites peuvent impliquer plusieurs parties prenantes et experts. Les méthodes qui peuvent être utilisées pour faire émerger des points de vue, au niveau des individus ou d'un groupe, sont décrites à l'Article B.1.

B.2.2 Listes de contrôle, classifications et taxonomies

B.2.2.1 Vue d'ensemble

Les listes de contrôle sont utilisées de différentes manières lors de l'appréciation du risque: elles participent par exemple à la compréhension du contexte, à l'identification des risques et à leur regroupement à différentes fins lors de l'analyse. Elles sont également utiles au management du risque, par exemple pour classer les moyens de maîtrise et les traitements, définir les responsabilités ou signaler les risques et en faire part aux personnes concernées.

Une liste de contrôle peut être basée sur l'expérience ou sur les échecs et réussites antérieurs, mais, de manière plus formelle, les typologies des risques et les taxonomies peuvent être développées pour catégoriser ou classer les risques en fonction d'attributs communs. Dans leurs formes pures, les typologies sont des systèmes de classification conceptuellement dérivée descendante, alors que les taxonomies sont des systèmes de classification dérivée de manière empirique ou théorique ascendante. Les formes hybrides font généralement appel à ces deux formes pures.

Les taxonomies des risques sont généralement destinées à être mutuellement exclusives et collectivement exhaustives (pour éviter les chevauchements et les écarts, par exemple). Les classifications des risques peuvent servir à isoler une catégorie spécifique de risques afin de l'examiner plus en détail.

Les typologies et les taxonomies peuvent être hiérarchiques et comporter plusieurs niveaux de classification. Il convient que toutes les taxonomies soient hiérarchiques et qu'il soit possible de les subdiviser en niveaux de résolution de plus en plus précis. Cela permettra de disposer d'un nombre gérable de catégories, tout en bénéficiant d'une précision suffisante.

B.2.2.2 Utilisation

Les listes de contrôle, les classifications et les taxonomies peuvent être conçues pour être appliquées au niveau stratégique ou opérationnel. Elles peuvent se matérialiser sous forme de questionnaires, entretiens, ateliers structurés ou combinaisons de ces trois éléments dans le cadre de discussions en face à face ou à l'aide d'outils informatisés.

Voici quelques exemples de listes de contrôle, classifications ou taxonomies fréquemment utilisées au niveau stratégique:

- AFOM (atouts, faiblesses, opportunités et menaces) identifie les facteurs, dans les contextes interne et externe, qui permettent de définir des objectifs et les stratégies destinées à les mettre en œuvre en tenant compte des risques.
- PESTLE, STEEP, STEEPLD, etc. sont des acronymes représentant les types de facteurs à prendre en compte lors de l'établissement du contexte ou de l'identification des risques [14]. Les lettres qui les composent représentent les mots Politique, Economique, Sociologique, Technologie, Ecologique, Légal, Ethique et Démographique. Il est possible de choisir les catégories pertinentes pour une situation donnée et d'élaborer des listes de contrôle pour différents exemples dans chaque catégorie.

- Prise en compte des objectifs stratégiques, des facteurs de réussite essentiels à la réalisation des objectifs, des menaces pesant sur les facteurs de réussite et de risque. Des traitements du risque et des indicateurs d'alerte précoces relatifs aux facteurs de risque peuvent être développés à partir de ce risque.

Au niveau opérationnel, les listes de contrôle répertoriant les dangers permettent d'identifier les dangers dans le cadre de l'analyse HAZID (identification des dangers) et de l'analyse préliminaire du danger (APD) [15]. Ces appréciations du risque de sécurité préliminaires sont généralement effectuées au début de la phase de conception d'un projet.

Il est possible de classer les risques selon les catégories générales suivantes:

- par source de risque: prix du marché, défaut de la contrepartie, fraude, dangers liés à la sécurité, etc.;
- en fonction des conséquences, des aspects ou de l'importance des objectifs ou des performances.

Il peut être utile de définir au préalable des catégories de risques afin de ne négliger aucun type de problème potentiel. Toutefois, il est difficile de garantir que ces catégories couvriront tous les risques possibles. En effet, lorsque les risques sont subdivisés en catégories prédéfinies, la réflexion s'y limite et certains aspects importants risquent d'être ignorés.

Les listes de contrôle, les typologies et les taxonomies sont utilisées avec d'autres techniques décrites dans le présent document, par exemple les mots clés de l'analyse HAZOP (B.2.4) et les catégories de l'analyse d'Ishikawa (B.3.3). L'IEC 62740:2015 présente un exemple de taxonomie pouvant être utilisé pour prendre en compte les facteurs humains lors de l'identification d'un risque [16].

En général, plus la liste de contrôle est spécifique, plus son utilisation dans le contexte particulier dans lequel elle a été élaborée est limitée. Les questions formulées de manière générale sont souvent plus efficaces pour stimuler la créativité lors de l'identification des risques.

B.2.2.3 Entrées

Données ou modèles à partir desquels des listes de contrôle, taxonomies ou classifications valides vont être élaborées.

B.2.2.4 Résultats

Les résultats prennent les formes suivantes:

- listes de contrôle, questions ou catégories et systèmes de classification;
- compréhension du risque consécutive à l'utilisation des éléments ci-dessus, y compris (dans certains cas) de listes et de regroupements de risques.

B.2.2.5 Avantages et limites

Les avantages des listes de contrôle, taxonomies et typographies incluent ce qui suit.

- Elles permettent à toutes les parties prenantes de comprendre les risques de la même manière.
- Si elles sont bien conçues, elles introduisent une vaste expertise dans un système facile à utiliser pour les profanes.
- Une fois élaborées, elles exigent peu d'expertise.

Les limites incluent ce qui suit.

- Leur utilisation est limitée dans les situations nouvelles pour lesquelles aucun historique utile n'existe ou aux situations qui diffèrent de celles pour lesquelles elles ont été élaborées.
- Elles traitent de points déjà connus ou imaginés.
- Elles sont souvent génériques et peuvent ne pas s'appliquer aux circonstances particulières considérées.
- Leur éventuelle complexité peut gêner l'identification des relations (interconnexions et autres regroupements possibles, par exemple).
- Le manque d'informations peut entraîner des chevauchements et/ou des écarts (lorsque les systèmes ne sont pas mutuellement exclusifs ni collectivement exhaustifs, par exemple).
- Elles peuvent encourager les comportements consistant à simplement cocher les cases plutôt que l'exploration d'idées.

B.2.2.6 Documents de référence

[17] BROUGHTON, Vanda, *Essential classification*

[18] BAILEY, Kenneth, *Typologies and taxonomies: An introduction to classification techniques*

[19] VDI 2225 Blatt 1, Konstruktionsmethodik- Technisch-wirtschaftliches Konstruieren - Vereinfachte Kostenermittlung, 1997 Beuth Verlag

B.2.3 Analyse des modes de défaillance et de leurs effets (AMDE) et analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC)

B.2.3.1 Vue d'ensemble

Lorsque la méthode AMDE est utilisée, une équipe subdivise du matériel, un système, un processus ou un mode opératoire en plusieurs éléments. Pour chaque élément, les possibilités de défaillance, ainsi que les causes et les effets des éventuelles défaillances, sont pris en compte. L'AMDE peut être suivie d'une analyse de criticité qui définit l'importance de chaque mode de défaillance (AMDEC).

Pour chaque élément, les informations suivantes sont enregistrées:

- sa fonction;
- la défaillance pouvant survenir (mode de défaillance);
- les mécanismes susceptibles d'entraîner ces modes de défaillance;
- la nature des conséquences d'une éventuelle défaillance;
- la nature anodine ou dangereuse de la défaillance;
- le moment où la défaillance peut être détectée et la manière dont elle est détectée;
- les dispositions intrinsèques prévues pour compenser la défaillance.

Pour l'analyse AMDEC, l'équipe chargée de l'étude classe chacun des modes de défaillance identifiés en fonction de sa criticité. Plusieurs méthodes de criticité différentes peuvent être utilisées. La matrice conséquence/vraisemblance qualitative, semi-quantitative ou quantitative (B.10.3) ou l'utilisation d'un degré de priorité du risque (RPN) sont les méthodes les plus fréquemment utilisées. Une mesure quantitative de la criticité peut également être dérivée des taux de défaillance réels et d'une mesure quantitative des conséquences lorsque ceux-ci sont connus.

NOTE Le RPN est une méthode basée sur des indices (B.8.6) qui prend le produit des classements associés aux conséquences de la défaillance, à sa vraisemblance et à l'aptitude à détecter le problème (détection). Une priorité élevée est attribuée à une défaillance en cas de difficulté de détection.

B.2.3.2 Utilisation

La méthode AMDE/AMDEC peut être appliquée lors de la conception, de la fabrication ou du fonctionnement d'un système physique afin d'apporter des améliorations pendant la phase de conception, de choisir entre plusieurs autres conceptions possibles ou de planifier un programme de maintenance. Elle peut également être appliquée aux processus et aux modes opératoires tels que les procédures médicales et les processus de fabrication. Elle peut être utilisée à n'importe quel niveau d'un système: schémas de blocs, composants d'un système, ou étapes d'un processus.

L'AMDE peut être utilisée pour fournir des informations aux techniques d'analyse, telles que l'analyse par arbre de panne. Elle peut constituer le point de départ d'une analyse de cause initiale.

B.2.3.3 Entrées

Le terme "entrées" couvre les informations relatives au système à analyser et aux éléments associés qui sont suffisamment précises pour permettre une analyse pertinente des risques qu'un élément puisse subir une défaillance et les conséquences d'une telle défaillance. Il peut s'agir de dessins ou d'organigrammes, de détails sur l'environnement dans lequel le système fonctionne et, le cas échéant, d'informations historiques sur les défaillances.

L'AMDE est normalement mise en œuvre par une équipe pluridisciplinaire composée d'experts du système en cours d'analyse et dirigée par un animateur formé. Il est important que l'équipe couvre tous les domaines d'expertise concernés.

B.2.3.4 Résultats

Les résultats de l'AMDE prennent différentes formes:

- une fiche de travail contenant les modes de défaillance, les effets, les causes et les moyens de maîtrise existants;
- une mesure de la criticité de chaque mode de défaillance (pour l'AMDEC) et la méthode utilisée pour la définir;
- toute action recommandée, par exemple concernant des analyses plus approfondies, des modifications de la conception ou l'intégration de fonctions aux plans d'essai.

L'AMDEC permet d'établir un classement qualitatif de l'importance des modes de défaillance, mais peut également fournir un résultat quantitatif si des données appropriées sur le taux de défaillance et les conséquences quantitatives sont utilisées.

B.2.3.5 Avantages et limites

Les avantages des analyses AMDE/AMDEC incluent ce qui suit.

- Elles peuvent s'appliquer très largement aux aspects humains et techniques liés aux systèmes, au matériel, aux logiciels et aux procédures.
- Elles permettent d'identifier les modes de défaillance, leurs causes et leurs effets sur le système, et de les présenter dans un format lisible.
- Elles permettent d'éviter des modifications coûteuses de l'équipement en service en identifiant les problèmes au début du processus de conception.
- Elles fournissent des informations aux programmes de maintenance et de surveillance en mettant en évidence les fonctions essentielles à surveiller.

Les limites incluent ce qui suit.

- L'AMDE peut uniquement être utilisée pour identifier les modes de défaillance unique, et non les combinaisons de modes de défaillance.

- Si les études ne sont pas convenablement contrôlées et mises au point, elles peuvent prendre du temps et être onéreuses.
- L'utilisation de l'AMDE peut se révéler difficile et fastidieuse pour les systèmes complexes à plusieurs couches.

B.2.3.6 Document de référence

[20] IEC 60812, *Analyse des modes de défaillance et de leurs effets (AMDE et AMDEC)*

B.2.4 Etudes de danger et d'exploitabilité (HAZOP)

B.2.4.1 Vue d'ensemble

Une étude HAZOP consiste en un examen structuré et systématique d'un processus, d'une procédure ou d'un système planifié ou existant, qui implique l'identification des écarts potentiels par rapport à la conception prévue et l'étude de leurs causes et conséquences possibles.

Lors d'un atelier formel, l'équipe d'étude:

- subdivise le système, le processus ou la procédure en éléments de plus petite taille;
- convient de la conception prévue pour chaque élément et définit les paramètres pertinents (tels que le débit ou la température dans le cas d'un système physique);
- applique successivement des mots-guides à chaque paramètre de chaque élément pour anticiper les écarts possibles par rapport à la conception prévue, écarts susceptibles d'entraîner des résultats non souhaitables;

NOTE Toutes les combinaisons de mots-guides ne sont pas pertinentes.

- convient de la cause et des conséquences de chaque situation et suggère la manière de les traiter;
- documente la discussion et convient des actions possibles pour traiter les risques identifiés.

Le Tableau B.1 donne des exemples de mots-guides couramment utilisés pour des systèmes techniques. Des mots-guides similaires tels que "trop tôt", "trop tard", "trop beaucoup", "trop peu – pas assez", "trop long", "trop court", "mauvaise direction", "mauvais objet", "mauvaise action" peuvent être utilisés pour identifier les modes d'erreur humaine.

Les mots-guides sont appliqués à des paramètres tels que:

- propriétés physiques d'un matériau ou d'un processus;
- conditions physiques (température ou vitesse, par exemple);
- indications temporelles;
- intention spécifiée d'un composant d'un système ou d'une conception (transfert d'informations, par exemple);
- aspects fonctionnels.

**Tableau B.1 – Exemple de mots-guides fondamentaux
et de leurs significations génériques**

Mot-guide	Définition
Aucun ou non	Le résultat prévu ne s'est pas produit ni même partiellement, ou absence de la condition prévue
Plus (supérieur)	Augmentation quantitative
Moins (inférieur)	Diminution quantitative
Autant que	Modification/Accroissement qualitatif (matériau supplémentaire, par exemple)
En partie	Modification/Diminution qualitative (un ou deux composants uniquement dans un mélange donné, par exemple)
Inverse/opposé	Contraire logique de la conception prévue (refoulement, par exemple)
Autre que	Remplacement total, l'événement qui survient est complètement différent (mauvais matériau, par exemple)
Tôt	Relatif à l'heure
Tard	Relatif à l'heure

B.2.4.2 Utilisation

A l'origine, les études HAZOP ont été mises au point pour analyser les systèmes de processus chimiques, mais elles ont été étendues à d'autres types de systèmes, notamment les systèmes de puissance mécaniques, électroniques et électriques, les systèmes logiciels, les changements organisationnels, le comportement humain ainsi que la conception et la révision des contrats juridiques.

Le processus HAZOP peut concerner toutes les formes d'écart par rapport à la conception prévue, à la suite de défaillances de conception, de composants, de modes opératoires et actions humaines planifiées. Il est le plus souvent utilisé pour améliorer une conception ou identifier les risques associés à une modification de la conception. D'une manière générale, il est réalisé à l'étape de la conception détaillée, lorsqu'un diagramme exhaustif du processus prévu et les informations associées sont disponibles, mais que des modifications peuvent encore être apportées à la conception. Toutefois, sa mise en œuvre peut suivre une approche progressive. Différents mots-guides sont alors utilisés au fur et à mesure des différentes phases de la conception. L'étude HAZOP peut également être réalisée lors du fonctionnement, mais les modifications nécessaires peuvent s'avérer coûteuses à ce stade.

B.2.4.3 Entrées

Le terme "entrées" couvre les informations actuelles relatives au système à revoir et aux spécifications de conception et de performances prévues. Pour le matériel, il peut s'agir de dessins, de fiches techniques, d'organigrammes, de diagrammes logiques et de maîtrise de processus, ainsi que de procédures de fonctionnement et de maintenance. Pour les éléments non matériels liés à l'analyse HAZOP, il peut s'agir de tout document décrivant les fonctions et éléments du système ou du mode opératoire en cours d'étude, par exemple des diagrammes organisationnels et des descriptions de poste, un projet de contrat ou un projet de mode opératoire.

Une étude HAZOP est généralement effectuée par une équipe multidisciplinaire. Il convient que cette équipe soit composée de concepteurs et d'opérateurs du système, ainsi que de personnes qui ne sont pas directement impliquées dans la conception ou dans le système, le processus ou le mode opératoire étudié. Il convient que le responsable ou l'animateur de l'étude soit formé à mener des études HAZOP et ait une certaine l'expérience dans ce domaine.

B.2.4.4 Résultats

Les résultats consistent en des comptes rendus de réunion(s) HAZOP mentionnant les écarts relatifs à chaque point de revue. Il convient que les enregistrements concernant chaque écart

comportent le mot-guide utilisé et les causes possibles de cet écart. Ils peuvent également indiquer les actions permettant de résoudre les problèmes identifiés et la personne responsable de les exécuter.

B.2.4.5 Avantages et limites

Les avantages de la méthode HAZOP incluent ce qui suit.

- Elle permet d'examiner un système, un processus ou un mode opératoire de manière systématique afin d'identifier comment celui-ci peut échouer à atteindre son objectif.
- Elle permet à une équipe multidisciplinaire de procéder à un examen détaillé et approfondi.
- Elle identifie les problèmes potentiels au stade de la conception d'un processus.
- Elle génère des solutions et des traitements du risque.
- Elle est applicable à un large éventail de systèmes, de processus et de modes opératoires.
- Elle permet de prendre en compte de manière explicite les causes et conséquences d'une erreur humaine.
- Elle permet de consigner par écrit le processus qui peut être utilisé pour effectuer les contrôles préalables.

Les limites incluent ce qui suit.

- Elle peut prendre beaucoup de temps et donc être onéreuse.
- Elle a tendance à être répétitive et à examiner plusieurs fois les mêmes questions, ce qui peut poser des problèmes de concentration.
- Elle nécessite un niveau élevé de documentation ou de spécification de système/processus et de mode opératoire.
- L'attention peut porter exclusivement sur la recherche de solutions plutôt que sur les raisons qui motivent une action (ceci peut être limité par une approche progressive).
- La discussion peut porter essentiellement sur des détails de conception et non sur des questions plus larges ou externes.
- Elle est limitée par le projet de conception et la conception elle-même, ainsi que par le domaine d'application et les objectifs imposés à l'équipe.
- Le processus repose en grande partie sur l'expertise des concepteurs, qui peuvent avoir du mal à rester suffisamment objectifs quant aux problèmes liés à leurs conceptions.

B.2.4.6 Document de référence

[21] IEC 61882, *Etudes de danger et d'exploitabilité (études HAZOP) – Guide d'application*

B.2.5 Analyse du scénario

B.2.5.1 Vue d'ensemble

L'analyse de scénario est le nom donné à une série de techniques impliquant le développement de modèles de prédiction de l'avenir. De manière générale, elle consiste à définir un scénario plausible et à imaginer ce qui pourrait se passer compte tenu des développements futurs possibles.

Pour les périodes à relativement court terme, elle peut extrapoler les événements à partir de ceux qui sont survenus dans le passé. Pour les périodes à plus long terme, l'analyse de scénario peut consister à mettre au point un scénario imaginaire, mais crédible, puis à étudier la nature des risques liés à celui-ci. Le plus souvent, elle est mise en œuvre par un groupe de parties prenantes dont l'expertise et les centres d'intérêt sont différents. L'analyse de scénario permet de définir en détail le ou les scénarios à étudier et d'explorer leurs

implications et les risques associés. Les changements envisagés sont généralement les suivants:

- les changements d'ordre technologique;
- les futures décisions possibles et leurs éventuelles conséquences;
- les besoins des différentes parties prenantes et dans quelle mesure ils peuvent évoluer;
- les changements macro-environnementaux (réglementation, caractéristiques sociodémographiques, etc.);
- les changements de l'environnement physique.

B.2.5.2 Utilisation

L'analyse de scénario est le plus souvent utilisée pour identifier les risques et étudier leurs conséquences. Elle peut s'appliquer aux niveaux stratégique et opérationnel, à l'ensemble de l'organisation ou à une partie de celle-ci.

L'analyse de scénario à long terme permet de planifier les principales évolutions, telles que celles qui sont intervenues au cours des 50 dernières années dans les domaines de la technologie, des préférences des consommateurs, des comportements sociaux, etc. L'analyse de scénario ne peut pas prévoir la probabilité de telles évolutions, mais peut étudier leurs conséquences et aider les organisations à développer les forces et la résilience nécessaires pour s'adapter aux changements prévisibles. Elle peut être utilisée pour anticiper l'évolution des menaces et opportunités, et peut s'appliquer à tous les types de risques.

L'analyse de scénario à court terme permet d'étudier les conséquences d'un événement initiateur. Des scénarios probables peuvent être extrapolés à partir de modèles ou de situations semblables survenues dans le passé. Exemples de scénarios à court terme: la planification des situations d'urgence ou les interruptions d'activité. Si aucune donnée n'est disponible, les opinions des experts sont utilisées, auquel cas il est très important de prêter une attention particulière à la manière dont ils expliquent leurs points de vue.

B.2.5.3 Entrées

Pour entreprendre une analyse de scénario, des données relatives aux tendances et évolutions actuelles et des idées de changements à mettre en place sont nécessaires. Pour les scénarios complexes ou à très long terme, des connaissances de la technique sont exigées.

B.2.5.4 Résultats

Le résultat peut prendre la forme d'une "histoire" décrivant, pour chaque scénario, la transition de la situation présente vers le scénario en question. Les effets étudiés peuvent présenter des avantages et des inconvénients. Ces histoires peuvent contenir des détails plausibles apportant de la valeur aux scénarios.

D'autres résultats peuvent être: une meilleure compréhension des effets possibles des politiques ou des plans relatifs aux événements futurs envisagés, une liste des risques pouvant survenir si ces événements devaient se produire et, dans certaines applications, une liste des indicateurs avancés associés à ces risques.

B.2.5.5 Avantages et limites

Les avantages de l'analyse de scénario incluent ce qui suit.

- Elle prend en compte un large éventail d'événements futurs possibles. Cette méthode peut être préférable à l'approche classique qui consiste à s'appuyer sur des prévisions selon lesquelles les événements à venir s'inscriront probablement dans la liste des tendances passées. Cet élément est important lorsque les connaissances actuelles sur lesquelles

reposent les prévisions sont limitées, ou lorsque les risques sont pris en compte à plus long terme.

- Elle est compatible avec une grande diversité de modes de pensée.
- Elle favorise la surveillance des indicateurs avancés de changement.
- Les décisions prises quant aux risques identifiés peuvent favoriser la résilience face à n'importe quel type de situation.

Les limites incluent ce qui suit.

- Il se peut que les scénarios utilisés ne reposent pas sur des fondements adéquats, par exemple si les données utilisées sont spéculatives. Cela pourrait conduire à des résultats irréalistes susceptibles de ne pas être interprétés comme tels.
- Il existe très peu d'éléments indiquant que les scénarios étudiés pour l'avenir à long terme se réalisent vraiment.

B.2.5.6 Documents de référence

[22] RINGLAND, Gill. *Scenarios in business*

[23] Van der HEIJDEN, Kees. *Scenarios: The art of strategic conversation*

[24] CHERMACK, Thomas J. *Scenario planning in organizations*

[25] MUKUL PAREEK, *Using Scenario analysis for managing technology risk*

B.2.6 Méthode SWIFT ("Que se passerait-il si?")

B.2.6.1 Vue d'ensemble

La méthode SWIFT est une technique d'identification des risques générale qui peut être utilisée ponctuellement ou dans le cadre d'une approche progressive (HAZOP ou AMDE) afin d'améliorer l'efficacité de méthodes ascendantes. Une séance de "brainstorming" structuré (B.1.2) est organisée dans le cadre d'un atelier formel où des mots-guides prédéfinis (durée, montant, etc.) sont combinés à des questions émanant des participants et commençant le plus souvent par une expression du type "Que se passerait-il si?" ou "Comment?". Elle est similaire à la méthode HAZOP, mais elle s'applique à un système ou à un sous-système plutôt qu'à la conception prévue.

Avant le début de l'étude, l'animateur prépare une liste de questions permettant de passer en revue l'ensemble des risques ou sources de risques. Au début de l'atelier, le contexte, le domaine d'application et l'objectif de l'étude SWIFT sont l'objet d'une discussion et les critères de réussite sont présentés en détail. A l'aide des mots-guides et des questions du type "Que se passerait-il si?", l'animateur invite les participants à se lever et à discuter de sujets tels que:

- les risques connus;
- les sources et les facteurs de risque;
- les expériences, réussites et incidents antérieurs;
- les moyens de maîtrise connus et existants;
- les exigences et contraintes réglementaires.

L'animateur utilise la liste de mots-guides pour orienter la discussion et soumet des questions et scénarios supplémentaires à la réflexion de l'équipe. L'équipe vérifie si les moyens de maîtrise sont adéquats et, si tel n'est pas le cas, envisage des traitements potentiels. Lors de la discussion, d'autres questions du type "Que se passerait-il si?" sont posées.

Dans certains cas, des risques spécifiques sont identifiés et une description du risque, de ses causes, de ses conséquences et de ses moyens de maîtrise peut être enregistrée. En outre, d'autres sources ou facteurs de risque, d'autres problèmes liés aux moyens de maîtrise ou d'autres questions d'ordre général peuvent être identifiés.

Lorsqu'une liste de risques est générée, une méthode d'appréciation du risque qualitative ou semi-quantitative est souvent utilisée pour classer les actions définies en matière de niveau de risque. Les moyens de maîtrise existants et leur efficacité sont généralement pris en compte.

B.2.6.2 Utilisation

Cette technique peut être appliquée de façon générale aux systèmes, aux éléments d'une installation, aux modes opératoires et aux organisations. En particulier, elle permet d'examiner les conséquences de certains changements et les risques ainsi modifiés ou créés. Les résultats positifs et négatifs peuvent être pris en compte. Cette technique peut également être utilisée pour identifier les systèmes ou les processus pour lesquels il vaudrait la peine d'investir des ressources dans une étude HAZOP ou AMDE plus précise.

B.2.6.3 Entrées

Une bonne compréhension du système, du mode opératoire, de l'élément de l'installation et/ou des changements et des contextes externe et interne est nécessaire. Ces informations sont établies à la suite d'entretiens, par la mise en place d'une équipe pluridisciplinaire et par l'étude de documents, de plans et de dessins par l'animateur. Afin de faciliter le processus d'analyse, le système étudié est normalement divisé en plusieurs éléments. Il est nécessaire que l'animateur soit formé à la méthode SWIFT, cette formation pouvant généralement être effectuée rapidement.

B.2.6.4 Résultats

Les résultats consistent en un registre des risques dans lequel les actions ou les tâches sont classées par risque. Ce registre peut servir de point de départ à un plan de traitement.

B.2.6.5 Avantages et limites

Les avantages de la méthode SWIFT incluent ce qui suit.

- Elle peut être largement appliquée à toutes les formes d'installation ou de système, de situation ou de circonstance, d'organisation ou d'activité.
- Elle demande peu de préparation par l'équipe.
- Elle est relativement rapide et les principaux risques et sources de risques apparaissent rapidement au cours de l'atelier.
- L'étude est "orientée système" et permet aux participants de voir comment le système réagit aux écarts, plutôt que de simplement examiner les conséquences de la défaillance d'un composant.
- Elle peut être utilisée pour identifier les opportunités d'amélioration des processus et des systèmes et, d'une manière générale, pour identifier les actions entraînant et augmentant les chances de conséquences favorables.
- Elle permet d'impliquer dans l'atelier les personnes responsables des moyens de maîtrise existants et des actions supplémentaires de traitement du risque, et d'accroître leurs responsabilités.
- Elle permet de créer un registre des risques et un plan de traitement du risque sans gros effort supplémentaire.

Les limites incluent ce qui suit.

- Si l'expérience de l'équipe n'est pas suffisante ou que le système de questions n'est pas complet, certains risques ou dangers peuvent ne pas être identifiés.
- L'application de la technique générale peut ne pas révéler les causes complexes, détaillées ou corrélées.

- Les recommandations sont souvent génériques: la méthode risque de ne pas proposer de moyens de maîtrise solides et détaillés sans analyse plus poussée, par exemple.

B.2.6.6 Document de référence

- [26] CARD, Alan J. WARD, James R. and CLARKSON, P. John. Beyond FMEA: The structured what-if technique (SWIFT)

B.3 Techniques de détermination des sources, causes et facteurs de risque

B.3.1 Généralités

La compréhension des causes des événements possibles et des facteurs de risque peut être utilisée pour mettre au point des stratégies permettant d'éviter les conséquences défavorables ou pour renforcer celles qui sont positives. Souvent, il existe une hiérarchie des causes composée de plusieurs niveaux avant d'atteindre la cause initiale. D'une manière générale, les causes sont analysées jusqu'à ce que des actions puissent être déterminées et justifiées.

Les techniques d'analyse des causes peuvent explorer les perceptions d'une cause dans une série de rubriques prédéfinies comme dans la méthode d'Ishikawa (B.3.3), ou elles peuvent adopter une approche qui s'appuie davantage sur la logique comme dans l'analyse par arbre de panne et dans l'analyse par arbre de réussite (voir B.5.7).

L'analyse "nœud papillon" (voir B.4.2) peut être utilisée pour représenter les causes et les conséquences de manière graphique, et pour montrer de quelle manière elles sont maîtrisées.

Plusieurs de ces techniques, décrites dans l'IEC 62740 [16], peuvent être utilisées de manière proactive pour analyser les causes possibles des événements qui pourraient survenir ultérieurement, ainsi que ceux qui se sont déjà produits. Ces techniques ne sont pas répétées ici.

B.3.2 Approche cindynique

B.3.2.1 Vue d'ensemble

La cindynique signifie littéralement la science du danger. L'approche cindynique identifie les sources et les facteurs de risque intangibles qui pourraient donner lieu à des conséquences nombreuses et variées. En particulier, elle définit et analyse:

- les incohérences, les ambiguïtés, les omissions, les lacunes (appelées "déficits"); et
- les divergences entre les parties prenantes (appelées "dissonances").

L'approche cindynique démarre par une collecte d'informations sur le système ou l'organisation à l'étude, ainsi que sur la situation cindynique définie par un espace géographique, temporel et chronologique et par un ensemble de réseaux ou de groupes de parties prenantes.

Elle utilise ensuite des entretiens semi-structurés (voir B.1.5) pour rassembler des informations à différents moments ($t_1, t_2, \dots, t_i$) concernant l'état de la connaissance et l'état d'esprit de chaque partie prenante, par rapport aux cinq critères cindyniques ci-dessous:

- les objectifs (but principal de l'organisation);
- les valeurs (que les parties prenantes tiennent en haute estime);
- les règles (droits, normes, procédures, etc. qui régissent ses accomplissements);
- les données (sur lesquelles s'appuie la prise de décision);

- les modèles (techniques, organisationnels, humains, etc. qui utilisent les données pour les prises de décisions).

NOTE Les éléments qui caractérisent les contextes internes et externes peuvent être rassemblés selon les cinq critères cindyniques.

Cette approche tient compte des perceptions autant que des faits.

Lorsque ces informations sont obtenues, la cohérence entre les objectifs à atteindre et les cinq critères cindyniques est analysée, et des tableaux sont créés pour répertorier les déficits et les dissonances.

B.3.2.2 Utilisation

L'objet de l'approche cindynique est de comprendre pourquoi, malgré toutes les mesures de contrôle prises pour les éviter, des sinistres continuent de se produire. L'approche a ensuite été élargie pour améliorer l'efficacité économique des organisations. Cette technique recherche les sources et facteurs de risque systémiques au sein d'une organisation, lesquels peuvent avoir des conséquences très variées. Elle s'applique à un niveau stratégique et peut être utilisée pour identifier les facteurs qui agissent de manière favorable ou défavorable pendant l'évolution du système pour atteindre de nouveaux objectifs.

Elle peut également être utilisée pour valider la cohérence de tout projet, et elle est particulièrement utile dans l'étude des systèmes complexes.

B.3.2.3 Entrées

Les informations décrites ci-dessus. L'analyse implique habituellement une équipe multidisciplinaire qui comprend des personnes ayant une réelle expérience opérationnelle, ainsi que les personnes qui déploient les moyens de traitement pour lutter contre les sources de risques identifiées.

B.3.2.4 Résultats

Les résultats sont des tableaux qui indiquent les déficits et les dissonances entre les parties prenantes (voir exemples ci-dessous). Le Tableau B.2 représente une matrice qui indique les déficits de chaque partie prenante par rapport aux cinq axes d'analyse (objectif, valeurs, règles, modèles et données). En comparant les informations rassemblées sous forme d'entrées entre les situations aux moments t_1 , t_2 , ..., t_i , il est possible d'identifier les déficits entre différentes situations.

Tableau B.2 – Tableau des déficits pour chaque partie prenante

Partie prenante	Critère d'analyse				
	Objectifs	Valeurs	Règles	Données	Modèles
S1		Met l'accent sur un nombre de valeurs restreint	Absence de référence aux procédures	Absence de référence aux mesures	Absence de référence aux modèles
S2	Incohérence entre les objectifs et les règles	Manque de hiérarchie entre les valeurs	Manque de hiérarchie entre les règles	Ignorance de l'expérience et du retour des autres pays	Ignorance des modèles spécifiques
S3	Incohérence entre les objectifs et les normes	Met l'accent sur une valeur spécifique (par exemple, l'emploi)	Manque de hiérarchie entre les règles	Aucune attention aux données spécifiques (par exemple, les accidents du travail)	Manque de hiérarchisation lors du choix des modèles

Le Tableau B.3 est une matrice où les parties prenantes pertinentes sont représentées sur les deux axes et où les différences de point de vue entre les parties prenantes (dissonances) apparaissent dans les cellules de la matrice. Ces tableaux permettent d'établir un programme de réduction des déficits et des dissonances.

Tableau B.3 – Tableau des dissonances entre les parties prenantes

Partie prenante	Partie prenante			
	S1	S2	S3	S4
S1		S1 et S2 ne partagent pas les mêmes objectifs	S1 et S3 ne partagent pas les mêmes valeurs	S1 et S4 ne partagent pas les mêmes systèmes de mesure
S2			S2 et S3 ne s'accordent pas dans l'interprétation des procédures	S2 et S4 ne s'accordent pas sur les données
S3				S3 et S4 sont en désaccord sur l'interprétation des règles
S4				

B.3.2.5 Avantages et limites

Les avantages de l'approche cindynique incluent ce qui suit.

- Il s'agit d'une approche systémique, multidimensionnelle et multidisciplinaire.
- Elle fournit une connaissance du potentiel de risque d'un système et de sa cohérence.
- Elle tient compte des aspects humains et organisationnels des risques à tous les niveaux de responsabilité.
- Elle intègre les notions d'espace et de temps.
- Elle produit des solutions pour réduire les risques.

Les limites incluent ce qui suit.

- Elle ne tente pas de hiérarchiser les sources de risques ni les risques.
- L'industrie vient à peine de commencer à utiliser cette approche. Par conséquent, elle ne bénéficie pas de la maturité acquise par les approches classiques au cours des développements passés.
- Selon le nombre de parties prenantes impliquées, elle peut mobiliser beaucoup de temps et de ressources.

B.3.2.6 Documents de référence

[27] KERVERN, G-Y. Elements fondamentaux des cindyniques

[28] KERVERN, G-Y. Latest advances in cindynics

[29] KERVERN, G-Y. & BOULENGER, P. Cindyniques – Concepts et mode d'emploi

B.3.3 Méthode d'Ishikawa (diagramme en arêtes de poisson)

B.3.3.1 Vue d'ensemble

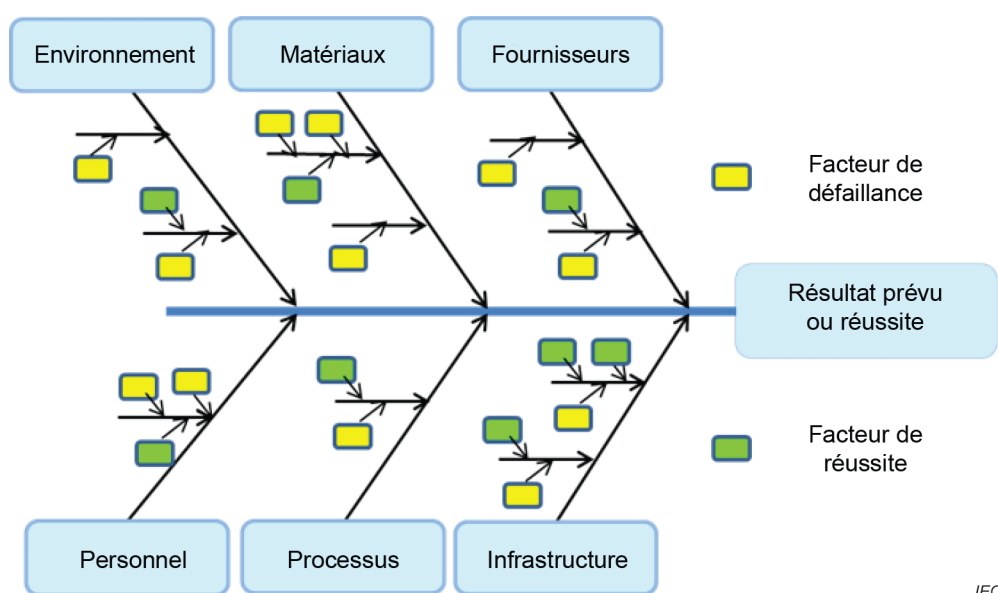
L'analyse d'Ishikawa s'appuie sur une approche en équipe pour identifier les causes possibles d'un effet, d'un événement, d'une question ou d'une situation souhaitable ou non souhaitable. Les facteurs contributifs sont classés en grandes catégories afin de couvrir les causes humaines, techniques et organisationnelles. Les informations sont représentées sous la forme

d'un diagramme en arêtes de poisson, également appelé "diagramme d'Ishikawa" (voir Figure B.1). Les principales étapes de réalisation de l'analyse sont les suivantes:

- Établir l'effet à analyser et le mettre dans une case en tête du diagramme en arêtes de poisson. L'effet peut être positif (un objectif) ou négatif (un problème).
- S'accorder sur les principales catégories de causes. Exemples de catégories couramment utilisées:
 - 6 M, par exemple méthodes, machines, milieu, matières, main d'œuvre, moyens;
 - matières, méthodes et processus, environnement, équipement, personnes, mesures;

NOTE Tous les ensembles de catégories convenus en fonction des circonstances analysées peuvent être utilisés. La Figure B.1 représente une autre possibilité.

- Demander "pourquoi?" et "comment cela pourrait-il se produire?" de manière répétitive pour explorer les causes et les facteurs influents dans chaque catégorie, et les ajouter aux arêtes du poisson.
- Revoir tous les nœuds pour vérifier la cohérence et l'exhaustivité et s'assurer que les causes s'appliquent au principal effet.
- Identifier les facteurs les plus importants en fonction de l'avis de l'équipe et des preuves disponibles.



IEC

Figure B.1 – Exemple de diagramme d'Ishikawa (en arêtes de poisson)

Le diagramme est souvent établi selon un scénario d'atelier.

B.3.3.2 Utilisation

L'analyse d'Ishikawa peut être utilisée pour l'analyse de cause initiale d'événements qui ont eu lieu ou pour identifier les facteurs qui pourraient contribuer à des résultats qui n'ont pas encore été obtenus. La méthode peut être utilisée pour examiner des situations à tous les niveaux d'une organisation et sur toutes les échelles de temps.

Les diagrammes sont en général utilisés de manière qualitative. Il est possible d'attribuer des probabilités attribuées aux causes génériques, puis aux sous-causes en fonction du degré de conviction sur leur pertinence. Toutefois, les facteurs contributifs interagissent souvent et participent aux effets de manière complexe, et il peut y avoir des causes non identifiées, ce qui rend la quantification non valide.

B.3.3.3 Entrée

Les entrées sont l'expertise et l'expérience des participants, ainsi que la compréhension de la situation examinée.

B.3.3.4 Résultat

Les résultats sont les causes perçues de l'effet analysé, normalement présentées dans un diagramme en arêtes de poisson ou diagramme d'Ishikawa. Le diagramme d'Ishikawa est structuré en représentant les catégories principales par les lignes partant de la colonne vertébrale du poisson, avec des nœuds et des sous-nœuds décrivant les sous-causes plus spécifiques se trouvant dans ces catégories.

B.3.3.5 Avantages et limites

Les avantages de la technique d'Ishikawa incluent ce qui suit.

- Elle encourage la participation et utilise les connaissances du groupe.
- Elle fournit une approche concentrée pour le "brainstorming" ou d'autres techniques d'identification semblables.
- Elle peut s'appliquer à des situations très variées.
- Elle offre une analyse structurée de la cause, avec un résultat graphique facile à lire.
- Elle permet à chacun de signaler les problèmes dans un environnement neutre.
- Elle peut être utilisée pour identifier les facteurs contributifs à l'origine des effets souhaités et non souhaités.

NOTE Une atmosphère positive peut encourager une plus grande implication et participation.

Les limites incluent ce qui suit.

- La classification des facteurs de causalité en catégories principales a lieu au début de l'analyse et, de ce fait, les interactions entre les catégories pourraient ne pas être prises en compte de manière adéquate.
- Les causes potentielles qui ne sont pas couvertes par les catégories choisies ne sont pas identifiées.

B.3.3.6 Document de référence

[30] ISHIKAWA, K. Guide to Quality Control

Voir aussi l'IEC 62740 [16] pour trouver d'autres techniques d'analyse des causes.

B.4 Techniques d'analyse des moyens de maîtrise

B.4.1 Généralités

Les techniques décrites dans l'Article B.4 peuvent être utilisées pour vérifier que les moyens de maîtrise sont appropriés et adéquats.

L'analyse "nœud papillon" (B.4.2) et la méthode LOPA (B.4.4) identifient les barrières entre une source de risque et ses conséquences possibles; elles peuvent être utilisées pour vérifier que les barrières sont suffisantes.

L'analyse HACCP (B.4.3) recherche les points d'un processus où les conditions peuvent être surveillées et où des moyens de maîtrise peuvent être introduits lorsqu'une indication signale que les conditions varient.

L'analyse par arbre d'événement (B.5.6) peut également être utilisée comme outil d'analyse quantitative des moyens de maîtrise en calculant l'influence des différents moyens de maîtrise sur la probabilité des conséquences.

Toutes les techniques d'analyse de cause peuvent servir de base pour vérifier que chaque cause est maîtrisée.

B.4.2 Analyse "nœud papillon"

B.4.2.1 Vue d'ensemble

Un "nœud papillon" est une représentation graphique de vecteurs allant des causes d'un événement à ses conséquences. Il montre les moyens de maîtrise qui font varier la vraisemblance de l'événement et ceux qui font varier ses conséquences, si l'événement se produit. Il peut être considéré comme une représentation simplifiée d'un arbre de panne ou d'un arbre de réussite (analysant la cause d'un événement) et d'un arbre d'événement (analysant ses conséquences). Les diagrammes "nœud papillon" peuvent être conçus à partir d'arbres de pannes et d'événements, mais sont le plus souvent établis directement par une équipe selon un scénario d'atelier.

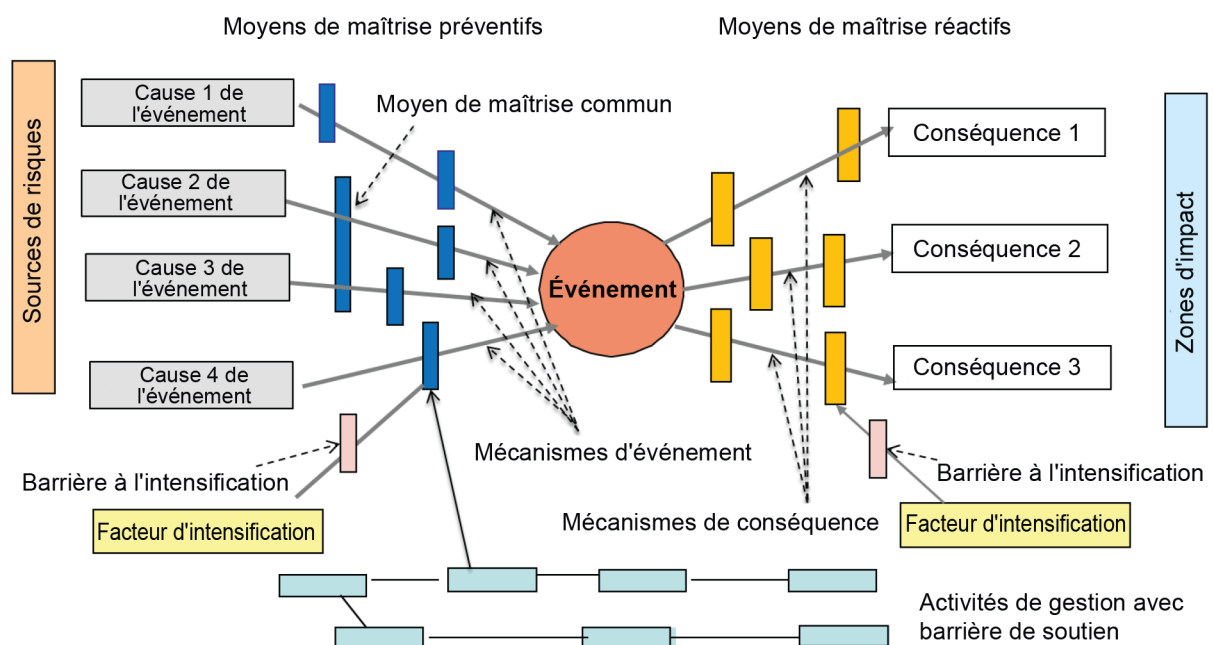


Figure B.2 – Exemple de "nœud papillon"

La procédure est la suivante.

- L'événement pris en compte est représenté par le nœud central du nœud papillon, voir Figure B.2.
- Les sources de risques (ou de dangers/menaces dans le contexte de la sécurité) sont situées à gauche du nœud et reliées au nœud par des lignes qui représentent les différents mécanismes par lesquels les sources de risques peuvent conduire à l'événement.
- Les barrières ou les moyens de maîtrise correspondant à chaque mécanisme sont représentés par des barres verticales qui traversent les lignes.
- À droite du nœud, des lignes sont tracées de l'événement à chaque conséquence potentielle.
- Après l'événement, les barres verticales représentent les moyens de maîtrise ou les barrières utilisé(e)s en réaction pour faire varier les conséquences.

- Les facteurs qui pourraient être à l'origine de la défaillance des moyens de maîtrise (facteurs d'intensification) sont ajoutés, ainsi que les moyens de maîtrise relatifs aux facteurs d'intensification.
- Les fonctions de gestion qui prennent en charge les moyens de maîtrise (formation et inspection par exemple) peuvent être représentées dans le diagramme "nœud papillon" et reliées au moyen de maîtrise correspondant.

Certains niveaux de quantification d'un diagramme "nœud papillon" peuvent être possibles si les vecteurs sont indépendants, si la probabilité d'une conséquence ou d'un résultat particulier est connue et si la probabilité qu'un moyen de maîtrise soit défaillant peut être chiffrée. Toutefois, dans de nombreux cas, les vecteurs et barrières ne sont pas indépendants, et les moyens de maîtrise peuvent être procéduraux et leur efficacité incertaine. La quantification est souvent plus appropriée en utilisant l'analyse par arbre de panne (B.5.7) et l'analyse par arbre d'événement (B.5.6) ou la méthode LOPA (B.4.4).

B.4.2.2 Utilisation

L'analyse "nœud papillon" est utilisée pour afficher et communiquer des informations concernant les risques dans les situations où les causes et les conséquences d'un événement sont diverses. Elle peut être utilisée pour explorer en détail les causes et les conséquences d'événements enregistrés sous une forme simple, dans un registre des risques (B.10.2). Elle est utilisée en particulier pour analyser les événements qui ont les conséquences les plus graves. Un "nœud papillon" est utilisé pendant l'évaluation des moyens de maîtrise pour vérifier que chaque vecteur allant de la cause à l'événement et de l'événement à la conséquence dispose d'un moyen de maîtrise efficace, et que les facteurs pouvant faire échouer ces moyens de maîtrise (y compris les défaillances des systèmes de gestion) sont reconnus. Il peut servir de base aux moyens d'enregistrer les informations concernant un risque qui ne correspond pas à la représentation linéaire simple d'un registre des risques. Il peut être utilisé proactivement pour envisager les événements potentiels et aussi rétrospectivement pour modéliser les événements qui se sont déjà produits.

L'analyse "nœud papillon" est utilisée lorsque la situation ne justifie pas la complexité d'une analyse par arbre de panne et par arbre d'événement complète, mais qu'elle est plus complexe que ce qu'un vecteur cause-événement-conséquence simple peut représenter.

Dans certaines situations, une analyse "nœud papillon" en cascade peut être développée; les conséquences d'un événement deviennent alors les causes de l'événement suivant.

B.4.2.3 Entrée

Les entrées comprennent des informations concernant les causes et les conséquences de l'événement prédéfini, et les moyens de maîtrise pouvant les faire varier. Ces informations peuvent être dérivées soit du résultat des techniques utilisées pour identifier les risques et les moyens de maîtrise, soit de l'expérience des personnes.

B.4.2.4 Résultat

Le résultat est un diagramme simple qui représente les principaux vecteurs de risque, les moyens de maîtrise en place et les facteurs qui pourraient être à l'origine de la défaillance des moyens de maîtrise. Il montre également les conséquences potentielles et les mesures qui peuvent être prises après la survenance de l'événement, afin de les faire varier.

B.4.2.5 Avantages et limites

Les avantages de l'analyse "nœud papillon" incluent ce qui suit.

- Elle est simple à comprendre et donne une représentation graphique claire d'un événement et de ses causes et conséquences.

- Elle concentre l'attention sur les moyens de maîtrise supposés mis en place et sur leur efficacité.
- Elle peut être utilisée pour les conséquences souhaitables ou non souhaitables.
- Son utilisation ne nécessite pas un niveau élevé d'expertise.

Les limites incluent ce qui suit.

- L'analyse "nœud papillon" ne peut pas représenter une situation où les vecteurs allant des causes à l'événement ne sont pas indépendants (c'est-à-dire où l'arbre de panne contiendrait des portes ET).
- Elle peut simplifier de manière excessive des situations complexes, particulièrement en cas de quantification.

B.4.2.6 Documents de référence

- [31] LEWIS, S. SMITH, K., *Lessons learned from real world application of the bow-tie method* [31]
- [32] HALE, A. R., GOOSSENS L.H.J., ALE, B.J.M., BELLAMY L.A. POST J. *Managing safety barriers and controls at the workplace*
- [33] MCCONNELL, P. and DAVIES, M. *Scenario Analysis under Basel II*

B.4.3 Analyse des dangers – points critiques pour leur maîtrise (HACCP)

B.4.3.1 Vue d'ensemble

La méthode HACCP (Analyse des dangers – points critiques pour leur maîtrise) a été mise au point pour garantir la salubrité alimentaire du programme spatial de la NASA, mais elle peut être utilisée pour les processus et les activités non alimentaires. Cette technique offre une structure permettant d'identifier les sources de risques (dangers ou menaces) et de mettre en place des moyens de maîtrise dans toutes les parties pertinentes d'un processus pour l'en protéger. La méthode HACCP est utilisée aux niveaux opérationnels, bien que ses résultats puissent soutenir la stratégie générale d'une organisation. L'analyse HACCP prévoit de limiter les risques par le biais de moyens de surveillance et de maîtrise tout au long d'un processus, au lieu de procéder à une inspection à la fin du processus.

L'analyse HACCP repose sur les sept principes suivants:

- 1) identification des dangers, des facteurs qui influencent le risque et des mesures préventives possibles;
- 2) détermination des étapes du processus où la surveillance est possible et où le processus peut être maîtrisé pour limiter les menaces (points de maîtrise critiques ou PCC);
- 3) définition de limites critiques pour les paramètres à surveiller. En d'autres termes, pour assurer la maîtrise du risque, il convient que chaque PCC respecte un certain nombre de paramètres spécifiques;
- 4) définition des procédures de surveillance des limites critiques de chaque PCC à intervalles déterminés;
- 5) mise en place d'actions correctives à utiliser lorsque le processus sort des limites établies;
- 6) mise en place des procédures de vérification;
- 7) tenue des archives et procédures de documentation correspondant à chacune des étapes.

B.4.3.2 Utilisation

L'analyse HACCP est une exigence dans la plupart des pays, en ce qui concerne les organisations officiant dans toute la chaîne alimentaire, de la récolte à la consommation, pour maîtriser les risques liés aux polluants physiques, chimiques ou biologiques.

Son utilisation a été étendue à la fabrication des produits pharmaceutiques et des appareils médicaux, ainsi qu'à d'autres secteurs où les risques biologiques, chimiques et physiques sont inhérents à l'organisation.

La technique consiste à identifier les sources de risques liées à la qualité de la production d'un processus, et à définir les points de ce processus où les paramètres critiques peuvent être surveillés et où les sources de risques peuvent être maîtrisées. Elle peut être généralisée à de nombreux autres processus, y compris par exemple aux processus financiers.

B.4.3.3 Entrées

Les entrées sont les suivantes:

- un organigramme de base ou un schéma de procédé;
- des informations sur les sources de risques susceptibles d'avoir un impact sur la qualité, la sécurité ou la fiabilité du produit ou du résultat du processus;
- des informations sur les points du processus, où les indicateurs peuvent être surveillés et où des moyens de maîtrise peuvent être introduits.

B.4.3.4 Résultats

Les résultats comprennent des archives incluant une fiche d'analyse de danger et un plan HACCP.

Les listes de fiches d'analyse de danger répertorient les éléments ci-dessous pour chaque étape du processus:

- les dangers susceptibles de se produire, d'être maîtrisés ou aggravés à cette étape;
- si les dangers représentent un risque important (basés sur l'étude des conséquences et de la probabilité d'occurrence et déterminés en s'appuyant sur l'expérience, les données et des documents techniques);
- les raisons du niveau d'importance attribué;
- les possibles mesures de prévention pour chaque danger;
- si les mesures de surveillance ou de maîtrise peuvent être appliquées à cette étape (en d'autres termes, s'il s'agit d'un PCC).

Le plan HACCP détermine la procédure à suivre pour contrôler une conception, un produit, un processus ou un mode opératoire spécifique. Le plan comprend une liste de tous les PCC, et pour chacun d'eux:

- les limites critiques correspondant à des mesures de prévention;
- les activités de surveillance et de maîtrise continue (notamment les éléments qui vont être surveillés et contrôlés, comment et quand ils vont l'être, et par qui);
- les actions correctives si des écarts par rapport aux limites critiques sont détectés;
- les activités de vérification et de tenue des archives.

B.4.3.5 Avantages et limites

Les avantages de l'analyse HACCP incluent ce qui suit.

- L'analyse HACCP est un processus structuré témoignant de la réalisation du contrôle qualité, ainsi que de l'identification et de la réduction des risques.
- Elle porte sur les aspects pratiques liés à la manière dont les sources de risques peuvent être localisées dans un processus, et le risque maîtrisé.

- Elle offre un contrôle des risques tout au long d'un processus, plutôt qu'un contrôle du produit fini.
- Elle attire l'attention sur les risques liés aux actions humaines et sur la manière de les maîtriser à l'endroit même où ils peuvent se produire, ou ultérieurement.

Les limites incluent ce qui suit.

- La méthode HACCP nécessite d'identifier les dangers, les risques qu'ils représentent et leur importance, perçus comme des entrées dans le processus. Il est également nécessaire de définir des moyens de maîtrise appropriés. La méthode HACCP pourrait nécessiter d'être combinée à d'autres outils permettant d'obtenir ces entrées.
- Il convient que les variations progressives des paramètres de maîtrise qui ont une importance statistique donnent lieu à une action, mais elles peuvent y échapper lorsque l'action est déclenchée seulement par le dépassement des limites définies pour ces paramètres.

B.4.3.6 Documents de référence

- [34] ISO 22000, *Systèmes de management de la sécurité des denrées alimentaires – Exigences pour tout organisme appartenant à la chaîne alimentaire*
- [35] *Systèmes de qualité et de sécurité sanitaire des aliments – Manuel de formation sur l'hygiène alimentaire et le Système d'analyse des risques – Points critiques pour leur maîtrise (HACCP)*

B.4.4 Méthode LOPA

B.4.4.1 Vue d'ensemble

La méthode LOPA analyse la réduction du risque obtenue par un ensemble de moyens de maîtrise. Elle peut être considérée comme un cas particulier de l'analyse par arbre d'événement (B.5.6), et est parfois utilisée à la suite de la méthode HAZOP (B.2.4).

Une paire cause-conséquence est choisie dans une liste de risques identifiés et les niveaux de protection indépendants (IPL) sont identifiés. Un IPL est un dispositif, un système ou une action capable d'empêcher un scénario d'évoluer vers sa conséquence non souhaitable. Il convient que chaque IPL soit indépendant de l'événement de causalité ou de tout autre niveau de protection associé au scénario. Il convient également que chaque IPL soit auditable. Les IPL comprennent:

- les fonctions de conception;
- les dispositifs de protection physique;
- les systèmes de verrouillage et d'arrêt;
- les alarmes critiques et l'intervention manuelle;
- la protection physique après l'événement;
- les systèmes d'intervention d'urgence.

Les procédures et/ou les inspections normalisées n'ajoutent pas directement de barrières contre les défaillances. Par conséquent, il convient de ne pas les considérer comme des IPL. La probabilité de défaillance de chaque IPL est estimée et un ordre d'amplitude est calculé pour déterminer si la protection globale permet de réduire le risque à un niveau tolérable.

La fréquence d'occurrence de la conséquence non souhaitable peut être déterminée en combinant la fréquence de la cause initiatrice aux probabilités de défaillance de chaque IPL en tenant compte de chaque élément de modification conditionnel. (Par exemple, le fait qu'une personne soit présente et puisse être affectée est un élément de modification conditionnel.) Des ordres d'amplitude sont utilisés pour connaître les fréquences et les probabilités.

B.4.4.2 Utilisation

La méthode LOPA peut être utilisée de manière qualitative pour revoir les niveaux de protection entre un événement de causalité et une conséquence. Elle peut également être utilisée de manière quantitative pour allouer des ressources aux traitements, en analysant la réduction du risque obtenue par chaque niveau de protection. Elle peut s'appliquer aux systèmes avec un horizon temporel à court ou long terme; elle est habituellement utilisée pour traiter des risques opérationnels.

La méthode LOPA peut également être utilisée de manière quantitative pour la spécification des IPL et des niveaux d'intégrité de sécurité (SIL) pour les systèmes instrumentés décrits dans l'IEC 61508 (toutes les parties) et dans l'IEC 61511 (toutes les parties), ainsi que pour démontrer qu'un SIL spécifié a été atteint.

NOTE Un SIL est un niveau discret (parmi quatre niveaux possibles) permettant de spécifier le degré de fiabilité exigé pour un système lié à la sécurité. Le niveau 4 est associé au plus haut degré d'intégrité et le niveau 1 au degré le plus bas.

B.4.4.3 Entrées

Les entrées de la méthode LOPA sont les suivantes:

- les informations de base sur les sources, causes et conséquences des événements;
- les informations relatives aux moyens de maîtrise en place ou aux traitements suggérés;
- la fréquence de l'événement de causalité, les probabilités de défaillance des niveaux de protection, la mesure des conséquences et une définition du risque tolérable.

B.4.4.4 Résultats

Les résultats sont des recommandations de traitements supplémentaires et des estimations du risque résiduel.

B.4.4.5 Avantages et limites

Les avantages de la méthode LOPA incluent ce qui suit.

- Elle demande moins de temps et de ressources qu'une analyse par arbre d'événement ou qu'une appréciation du risque intégralement quantitative, mais elle est plus rigoureuse que des opinions qualitatives subjectives.
- Elle aide à identifier et à mettre l'accent sur les ressources des niveaux de protection les plus critiques.
- Elle permet d'identifier les opérations, les systèmes et les processus dont les dispositifs de protection sont insuffisants.
- Elle met l'accent sur les conséquences les plus graves.

Les limites de la méthode LOPA incluent ce qui suit.

- Elle met l'accent sur une paire cause-conséquence et un scénario à la fois; les interactions complexes entre les risques ou entre les moyens de maîtrise ne sont pas couvertes.
- Lorsqu'elle est utilisée de manière quantitative, elle pourrait ne pas tenir compte des défaillances de mode commun.
- Elle ne s'applique pas à des scénarios très complexes composés de plusieurs paires cause-conséquence ou d'un ensemble de conséquences ayant un impact sur les différentes parties prenantes.

B.4.4.6 Documents de référence

[36] IEC 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

[37] IEC 61511 (toutes les parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*

[38] *Layer of protection analysis – Simplified process risk assessment*

B.5 Techniques permettant de comprendre les conséquences et la vraisemblance

B.5.1 Généralités

Les techniques décrites dans l'Article B.5 visent à améliorer la compréhension des conséquences et de leur vraisemblance. D'une manière générale, les conséquences peuvent être explorées selon les méthodes suivantes:

- l'expérimentation, comme les études sur les cellules pour explorer les conséquences de l'exposition à des toxines, et dont les résultats sont appliqués aux risques sanitaires pour l'homme et pour l'environnement;
- les recherches concernant les événements passés, y compris les études épidémiologiques;
- la modélisation visant à déterminer la manière dont les conséquences se développent après un déclencheur, et comment celui-ci dépend des moyens de maîtrise en place. Il peut s'agir de modèles mathématiques ou technologiques et de méthodes logiques comme l'analyse par arbre d'événement (B.5.6);
- les techniques encourageant la pensée imaginative comme l'analyse de scénario (B.2.5).

La vraisemblance d'un événement ou d'une conséquence particulière peut être estimée par:

- l'extrapolation à partir des données de l'historique (à condition que l'historique contienne suffisamment de données pertinentes pour que l'analyse soit valable du point de vue statistique). Cela concerne particulièrement les occurrences nulles, où le fait qu'un événement ou une conséquence ne se soit encore jamais produit(e) ne permet pas de retenir l'hypothèse qu'il/elle se produira pas dans un avenir proche;
- la synthèse des données relatives au taux de défaillance ou de réussite des composants du système: à l'aide de techniques comme l'analyse par arbre d'événement (B.5.6), l'analyse par arbre de panne (B.5.7) ou l'analyse causes-conséquences (B.5.5);
- les techniques de simulation pour générer, par exemple, la probabilité des défaillances des équipements et des structures du fait du vieillissement et d'autres processus de dégradation.

Des experts peuvent être appelés à exprimer leur opinion sur les vraisemblances et les conséquences, en tenant compte des informations pertinentes et des données de l'historique. Il existe un certain nombre de méthodes formelles permettant d'obtenir des avis experts en rendant l'utilisation du jugement visible et explicite (voir l'Article B.1).

Une conséquence et sa vraisemblance peuvent être combinées pour donner un niveau de risque. Celui-ci peut être utilisé pour évaluer l'importance d'un risque en comparant le niveau de risque à un critère d'acceptabilité, ou pour classer les risques par ordre d'importance.

Les techniques permettant de combiner les valeurs qualitatives des conséquences et la vraisemblance comprennent les méthodes utilisant un indice (B.8.6) et les matrices conséquence/vraisemblance (B.10.3). Une mesure unique du risque peut également être produite à partir de la distribution de la probabilité des conséquences (voir par exemple VaR (B.7.2) et CVaR (B.7.3) et les courbes en S (B.10.4)).

B.5.2 Analyse bayésienne

B.5.2.1 Vue d'ensemble

Il est courant de rencontrer des problèmes qui présentent, à la fois, des données et des informations subjectives. L'analyse bayésienne permet d'utiliser les deux types d'informations pour prendre des décisions. L'analyse bayésienne s'appuie sur un théorème attribué au Révérend Thomas Bayes (1760). Dans sa forme la plus simple, le théorème de Bayes fournit une base probabiliste permettant de changer d'avis à la lumière de nouvelles preuves. Elle est généralement exprimée selon la Formule (1):

$$\Pr(A|B) = \frac{\Pr(B|A)\Pr(A)}{\Pr(B)} \quad (1)$$

où

$\Pr(A)$ est l'appréciation a priori de la probabilité de A ;

$\Pr(B)$ est l'appréciation a priori de la probabilité de B ;

$\Pr(A|B)$ est la probabilité de A étant donné que B s'est produit (appréciation a posteriori);

$\Pr(B|A)$ est la probabilité de B étant donné que A s'est produit.

Le théorème de Bayes peut être élargi pour englober plusieurs événements dans un espace échantillon donné.

Par exemple, l'hypothèse retenue est que nous souhaitons utiliser certaines données, D , afin d'enrichir notre compréhension (ou manque de compréhension) d'un risque. L'objectif est d'utiliser ces données pour apprécier le mérite relatif d'un nombre (N) d'hypothèses concurrentes et sans point commun, désigné par H_n (où $n = 1, 2, \dots, N$). Le théorème de Bayes peut alors être utilisé pour calculer la probabilité de la j^{e} hypothèse en utilisant la Formule (2):

$$\Pr(H_j | D) = \Pr(H_j) \left[\frac{\Pr(D | H_j)}{\sum \Pr(H_n) \Pr(D | H_n)} \right] \quad (2)$$

où $j = 1, 2, \dots, n$.

Cela montre qu'après la prise en compte des nouvelles données, la probabilité de l'hypothèse j [c'est-à-dire $\Pr(H_j|D)$] est obtenue en multipliant sa probabilité a priori $\Pr(H_j)$ par la fraction entre parenthèses.

Le numérateur de cette fraction est la probabilité d'obtenir ces données si la j^{e} hypothèse est vraie. Le dénominateur provient d'une "loi de la probabilité totale" (probabilité d'obtenir ces données si, l'une après l'autre, chaque hypothèse se vérifiait). Le dénominateur est le facteur de normalisation.

Une probabilité bayésienne peut être mieux appréhendée si elle est considérée comme le degré de croyance d'une personne en un certain événement, par opposition à la théorie classique reposant sur la preuve physique.

B.5.2.2 Utilisation

L'analyse bayésienne est un moyen de déduction qui s'appuie sur des données à la fois basées sur le jugement et empiriques. Les méthodes bayésiennes peuvent être développées pour permettre de déduire les paramètres au sein d'un modèle de risque mis au point pour un

contexte particulier, par exemple, la probabilité d'un événement, l'importance d'un événement ou la durée jusqu'à un événement.

Les méthodes bayésiennes peuvent être utilisées pour fournir une estimation a priori du paramètre considéré en fonction des croyances subjectives. Une distribution de la probabilité a priori est habituellement associée aux données subjectives, car elle représente des incertitudes dans l'état des connaissances. Un a priori peut être construit à partir de données subjectives uniquement ou en utilisant des données pertinentes provenant de situations semblables. Une estimation a priori peut offrir une prévision probabiliste de la vraisemblance d'un événement et cela peut être utile pour l'appréciation du risque, lorsqu'il n'existe aucune donnée empirique.

Les données observées concernant un événement peuvent être combinées avec la distribution a priori à l'aide de l'analyse bayésienne, afin de fournir une évaluation a posteriori du paramètre de risque considéré.

Le théorème de Bayes est utilisé pour intégrer de nouvelles preuves aux croyances a priori, afin de former une évaluation mise à jour.

L'analyse bayésienne peut fournir des estimations ponctuelles et d'intervalles pour le paramètre considéré. Ces évaluations capturent les incertitudes associées à la fois à la variabilité et à l'état de connaissance. L'analyse bayésienne est une alternative à l'approche fréquentiste classique qui représente la variation statistique aléatoire de la variable prise en compte.

Le modèle de probabilité qui étaye une analyse bayésienne dépend de l'application. Par exemple, un modèle de probabilité de Poisson pourrait être utilisé pour les événements comme les accidents, la non-conformité ou les retards de livraison, ou un modèle de probabilité binomiale pourrait être utilisé pour les éléments exceptionnels. Il est de plus en plus courant de construire un modèle de probabilité pour représenter les liens de causalité entre les variables sous la forme d'un réseau bayésien (B.5.3).

B.5.2.3 Entrées

Les entrées de l'analyse bayésienne sont les données basées sur le jugement et empiriques nécessaires pour structurer et pour quantifier le modèle de probabilité.

B.5.2.4 Résultats

Comme pour les statistiques classiques, l'analyse bayésienne fournit des évaluations, soit sous forme de chiffres simples, soit sous forme d'intervalles, du paramètre considéré; elle peut s'appliquer à des résultats très divers.

B.5.2.5 Avantages et limites

Les avantages sont les suivants.

- Les exigences inférentielles sont faciles à comprendre.
- Elle offre un mécanisme permettant d'utiliser les croyances subjectives concernant un problème.
- Elle offre un mécanisme permettant de combiner les croyances a priori avec de nouvelles données.

Les limites sont les suivantes.

- Elle peut produire des distributions a posteriori qui dépendent fortement du choix de l'a priori.

- La résolution de problèmes complexes peut avoir un coût élevé en matière de statistique et mobiliser de nombreuses ressources humaines.

B.5.2.6 Documents de référence

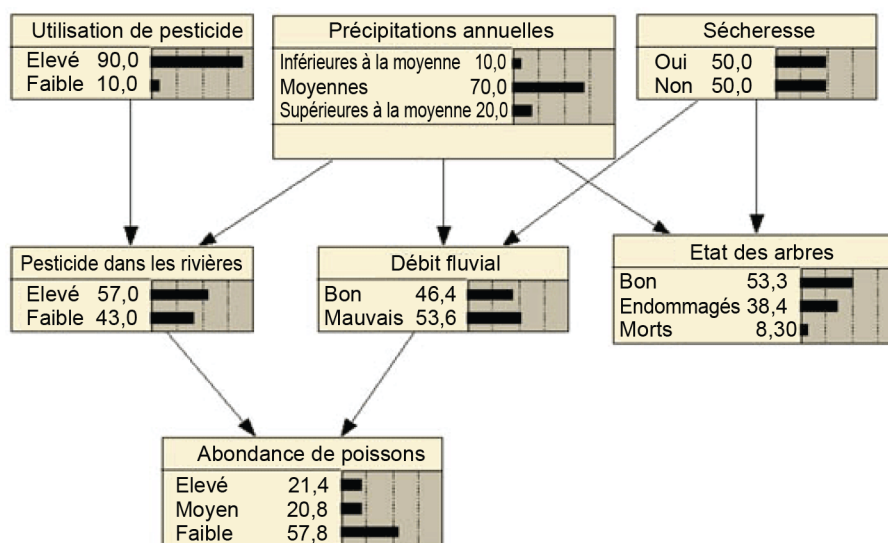
- [39] GHOSH, J., DELAMPADY, M. and SAMANTA, T. *An introduction to Bayesian analysis*, New York Springer-Verlag, 2006
- [40] QUIGLEY, J.L., BEDFORD, T.J. and WALLS, L.A. *Prior Distribution Elicitation*

B.5.3 Réseaux bayésiens et diagrammes d'influence

B.5.3.1 Vue d'ensemble

Un réseau bayésien (réseau de Bayes ou BN pour "Bayes' net") est un modèle graphique dont les nœuds représentent les variables aléatoires (discrètes et/ou continues) (Figure B.3). Les nœuds sont reliés par des arcs dirigés qui représentent les dépendances directes (qui sont souvent des relations de causalité) entre les variables.

Les nœuds qui pointent vers un nœud X sont appelés ses parents, et sont désignés $pa(X)$. La relation entre les variables est quantifiée par les distributions conditionnelles de la probabilité (DCP) associées à chaque nœud, désignées $P(X|pa(X))$, où l'état des nœuds enfants dépend de la combinaison des valeurs des nœuds parents. Dans la Figure B.3, les probabilités sont indiquées par des estimations ponctuelles.



IEC

Figure B.3 – Réseau bayésien montrant une version simplifiée d'un problème écologique réel: modélisation des populations de poissons autochtones dans l'Etat de Victoria en Australie

B.5.3.2 Utilisation

Un BN de base contient des variables qui représentent des événements incertains; il peut être utilisé pour estimer la vraisemblance ou le risque des conséquences spécifiées ou pour déduire les principaux facteurs de risque qui en sont à l'origine.

Un BN peut être élargi pour inclure les décisions, les actions et les valeurs, ainsi que les incertitudes, auquel cas il s'agit d'un diagramme d'influence qui peut être utilisé pour apprécier l'impact du moyen de maîtrise ou de la limitation des risques ou pour estimer les options d'intervention.

Un modèle de BN peut être construit comme une représentation qualitative d'un problème par les parties prenantes puis quantifié à l'aide de données pertinentes, même basées sur le

jugement (par exemple, une analyse du risque dans un centre de distribution de médicaments), ou un modèle de BN peut s'instruire à l'aide de données empiriques uniquement (par exemple, les moteurs de recherche sur Internet, les risques financiers). Quelle que soit la forme du BN, le mécanisme de déduction sous-jacent s'appuie sur le théorème de Bayes et possède les propriétés générales de l'analyse bayésienne (B.5.2).

Les BN sont utilisés dans une grande variété d'applications: y compris pour la prise de décision en matière d'environnement, pour les diagnostics médicaux, pour la prolongation de la durée de vie des infrastructures critiques, pour les risques de la chaîne logistique, pour la modélisation en image du développement d'un nouveau produit ou processus, pour la génétique, pour la reconnaissance vocale, pour l'économie, pour l'exploration spatiale et pour les moteurs de recherche sur Internet.

D'une manière générale, les BN offrent des modèles visuels qui favorisent l'articulation des problèmes et la communication entre les parties prenantes. Les modèles de BN permettent d'effectuer une analyse de sensibilité afin d'explorer les scénarios de type "que se passerait-il si?". La construction de la structure du BN qualitatif peut s'appuyer sur l'utilisation de la cartographie causale (B.6.1) et un BN peut être associé à une analyse de scénario (B.2.5) et à une analyse d'impacts croisés (B.6.2).

Les BN sont utiles pour obtenir les avis et l'accord des parties prenantes aux fins des décisions qui présentent des niveaux élevés d'incertitude et de divergence de points de vue entre les parties prenantes. La représentation est facilement compréhensible, bien qu'il soit exigé qu'elle soit produite par un expert.

Les BN peuvent être utiles pour cartographier des analyses de risques au bénéfice des parties prenantes non techniciennes, car ils favorisent la transparence des hypothèses et du processus, et traitent l'incertitude de manière mathématiquement correcte.

B.5.3.3 Entrées

Pour les BN, les entrées nécessitent une connaissance des variables d'un système (nœuds), les liens de causalité entre elles (arcs dirigés) et les probabilités a priori et conditionnelles de ces relations.

Dans le cas des diagrammes d'influence, les valeurs sont également nécessaires (par exemple, perte financière, blessures, etc.).

B.5.3.4 Résultats

Les BN offrent des distributions conditionnelles et marginales, dans un résultat graphique, généralement considérées comme des modèles à boîte noire faciles à interpréter, du moins par rapport à d'autres. Le modèle BN et les données peuvent facilement être modifiés pour visualiser aisément les relations et explorer la sensibilité des paramètres à différentes entrées.

B.5.3.5 Avantages et limites

Les avantages des BN incluent ce qui suit:

- Il existe des logiciels disponibles et relativement faciles à utiliser à comprendre.
- Leur cadre organisationnel est transparent et ils peuvent rapidement exécuter les scénarios et analyser la sensibilité du résultat aux différentes hypothèses.
- Ils peuvent inclure des croyances subjectives concernant un problème, ainsi que des données.

Les limites incluent ce qui suit.

- La définition de toutes les interactions est difficile dans les systèmes complexes, et elle peut devenir insoluble d'un point de vue informatique lorsque les tableaux de probabilité conditionnelle deviennent trop grands.
- Les BN sont souvent statiques et ne comprennent habituellement pas de boucle de rétroaction. Toutefois, l'utilisation de BN dynamiques est en augmentation.
- La définition des paramètres exige d'avoir connaissance de nombreuses probabilités conditionnelles qui sont généralement fournies par le jugement d'un expert. Les BN peuvent fournir des réponses uniquement à partir de ces hypothèses (une limite qui est commune à d'autres techniques de modélisation).
- Le résultat peut donner une réponse convaincante alors que l'utilisateur a saisi une erreur; la vérification des extrémités peut aider à localiser les erreurs.

B.5.3.6 Documents de référence

- [41] NEIL, Martin and FENTON, Norman. *Risk Assessment and Decision Analysis with Bayesian Networks* CRC Press, 2012
- [42] JENSEN, F.V., NIELSEN T. D. *Bayesian Networks and Decision Graphs*, 2nd ed. Springer, New York, 2007
- [43] NICHOLSON, A., WOODBERRY O and TWARDY C, The “Native Fish” Bayesian networks. *Bayesian Intelligence Technical Report 2010/3*, 2010
- [44] NETICA TUTORIAL

B.5.4 Analyse d'impact sur l'activité (AIA)

B.5.4.1 Vue d'ensemble

L'analyse d'impact sur l'activité propose d'analyser la manière dont les incidents et les événements pourraient avoir un impact sur les opérations d'une organisation, et d'identifier et de quantifier les aptitudes nécessaires à leur gestion. De manière spécifique, l'AIA propose une compréhension convenue:

- du caractère critique des processus métier clés, des fonctions et des ressources associées et des principales interdépendances qui existent au sein d'une organisation;
- de l'impact d'un sinistre sur la capacité et la possibilité d'atteindre des objectifs commerciaux essentiels;
- de la capacité et des aptitudes nécessaires pour gérer l'impact d'un sinistre et pour retrouver des volumes d'opérations acceptables.

L'AIA peut être entreprise à l'aide de questionnaires, d'entretiens, d'ateliers structurés ou d'une combinaison de ces trois éléments.

B.5.4.2 Utilisation

L'analyse d'impact sur l'activité permet de déterminer le caractère critique et les calendriers de remise en état pour les processus et les ressources associées (par exemple, les personnes, l'équipement et les technologies d'information), afin de pouvoir planifier correctement les opérations en cas d'événement paralysant. L'AIA facilite également la détermination des interdépendances et des relations entre les processus, les parties internes et externes et les liens de la chaîne logistique.

Elle peut également être utilisée dans le cadre de l'analyse des conséquences, pour la prise en compte des conséquences des événements paralysants.

L'AIA fournit des informations qui aident l'organisation à déterminer et à choisir les stratégies de continuité d'activité adéquates, permettant une réponse et une remise en état efficaces après un événement paralysant.

B.5.4.3 Entrées

Les entrées sont les suivantes:

- des informations concernant les objectifs, l'orientation stratégique, l'environnement, les actifs et les interdépendances de l'organisation;
- une vue d'ensemble des produits et services de l'organisation et de leur relation avec les processus métier;
- une appréciation des priorités d'après la revue de gestion des événements précédents;
- les caractéristiques des activités et opérations de l'organisation, y compris les processus, les ressources, les relations avec les autres organisations, les chaînes logistiques, les conventions d'externalisation et les différentes parties prenantes;
- des informations permettant d'apprécier les conséquences financières, légales et opérationnelles de la perte de processus critiques;
- un questionnaire préparé ou tout autre moyen de rassembler des informations;
- les résultats des autres appréciations de risques et analyses d'événements critiques liées aux résultats des incidents paralysants;
- la liste des personnes appartenant aux services pertinents de l'organisation et/ou des différentes parties prenantes à contacter.

B.5.4.4 Résultats

Les résultats sont les suivants:

- la liste des produits et services de l'organisation, par ordre de priorité;
- les documents qui décrivent les informations collectées comme entrées;
- une liste des processus critiques et des interdépendances associées, par ordre de priorité;
- les impacts documentés liés à une perte de processus critiques, y compris les impacts financiers, juridiques, environnementaux et opérationnels;
- les informations concernant les ressources et activités de soutien nécessaires pour rétablir les processus critiques;
- une appréciation des impacts au fil du temps, en cas d'arrêt de la fourniture de ces produits et services à court terme, à moyen terme et à long terme;
- les échéances concernant la reprise de la fourniture de ces produits et services à un niveau minimal spécifié, par ordre de priorité, en tenant compte des délais au-delà desquels les impacts de la non-reprise de la fourniture deviendraient inacceptables;
- les calendriers d'indisponibilité des processus critiques et les calendriers de remise en état des technologies d'information associées.

B.5.4.5 Avantages et limites

Les avantages de la méthode AIA incluent ce qui suit:

- une compréhension approfondie des processus critiques qui permettent à une organisation d'atteindre ses objectifs et qui indiquent les domaines où l'activité peut être améliorée;
- les informations nécessaires pour planifier la réponse d'une organisation en cas d'événement paralysant;
- la compréhension des principales ressources exigées en cas de sinistre;
- l'opportunité de redéfinir les processus opérationnels d'une organisation afin de contribuer à favoriser la résilience de l'organisation.

Les limites incluent ce qui suit:

- L'AIA s'appuie sur les connaissances et les perceptions des participants qui remplissent les questionnaires, ou qui assistent aux entretiens ou ateliers. Ceci peut conduire à des attentes simplistes ou trop optimistes concernant les exigences de remise en état.
- La dynamique de groupe peut avoir un impact négatif sur l'analyse exhaustive d'un processus critique.
- Les attentes concernant les exigences de remise en état peuvent être simplistes ou trop optimistes.
- Le niveau de compréhension adéquat des opérations et activités de l'organisation peut être difficile à obtenir.

B.5.4.6 Documents de référence

- [45] ISO/TS 22317, *Sécurité sociétale – Systèmes de management de la continuité d'activité – Lignes directrices pour l'analyse d'impact sur l'activité*
- [46] ISO 22301, *Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences*

B.5.5 Analyse causes-conséquences (ACC)

B.5.5.1 Vue d'ensemble

Dans certains cas, un événement qui pourrait être analysé par un arbre de panne est mieux couvert par l'ACC. Par exemple,

- s'il est plus facile de développer les séquences des conséquences que les relations causales;
- si l'AAP peut devenir trop volumineuse;
- si plusieurs équipes distinctes s'occupent des différentes parties de l'analyse.

En pratique, ce n'est souvent pas l'événement de tête qui est défini en premier, mais les événements potentiels à l'interface entre le domaine fonctionnel et le domaine technique.

L'événement "perte d'équipage ou de véhicule" lors d'une mission spatiale est pris comme exemple. Au lieu de construire un arbre de panne de grandes dimensions à partir de cet événement de tête, les événements non souhaitables intermédiaires comme la défaillance de la mise à feu ou la défaillance de la poussée peuvent être définis comme événements de tête et analysés comme des défaillances distinctes. Ces événements de tête sont ensuite utilisés comme entrées dans les arbres d'événements pour analyser leurs conséquences opérationnelles.

Deux types d'ACC peuvent être distingués, selon la partie de l'analyse qui est la plus pertinente pour les circonstances. Lorsque les causes décrites sont exigées, mais qu'une description plus générale de la conséquence est acceptable, alors la partie arbre de panne de l'analyse est développée et l'analyse est désignée par ACC-PEGP (petit arbre d'événement, grand arbre de panne). Lorsqu'une description détaillée des circonstances est exigée, mais que les causes peuvent être prises en compte moins en détail, l'analyse est désignée par ACC-GEPP (grand arbre d'événement, petit arbre de panne). La Figure B.4 représente un diagramme conceptuel d'une analyse causes-conséquences typique.

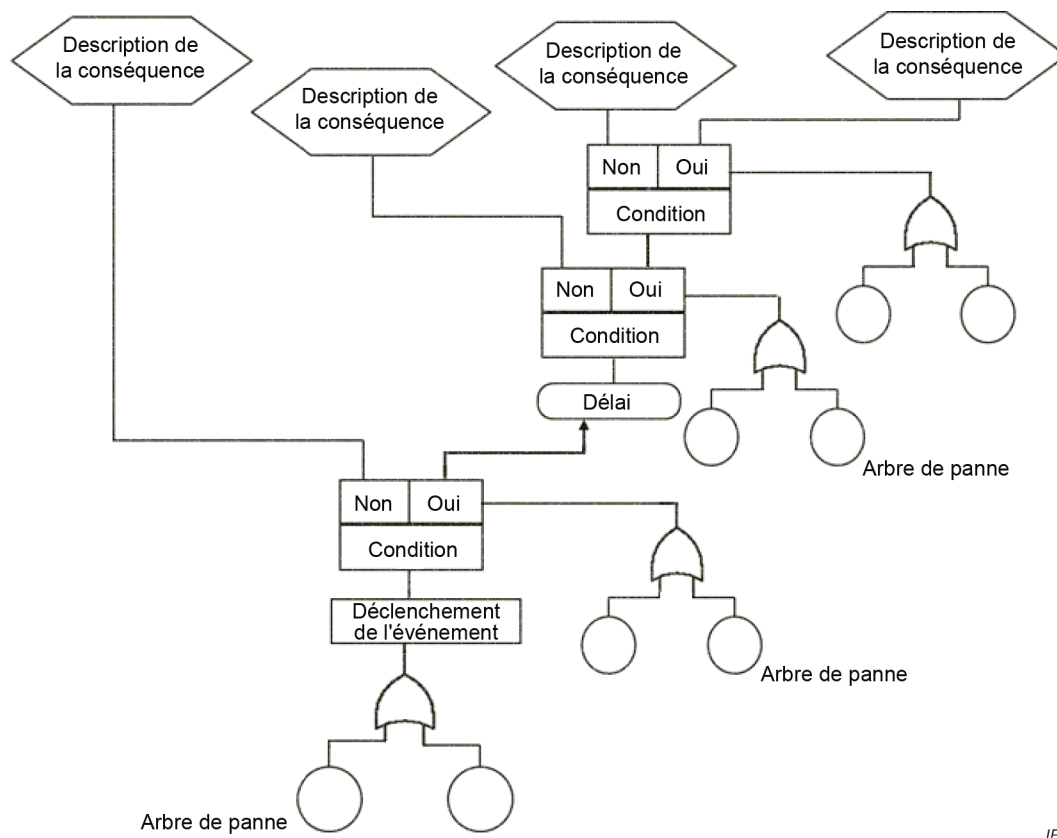
B.5.5.2 Utilisation

Comme l'analyse par arbre de panne, l'analyse causes-conséquences permet de représenter la logique de défaillance donnant lieu à un événement critique, mais ajoute à la fonctionnalité d'un arbre de panne en permettant l'analyse des défaillances chronologiques. La méthode permet également d'incorporer des actions différées dans l'analyse des conséquences, cela n'étant pas possible dans les arbres d'événements. Elle analyse les différents chemins dont dispose un système à la suite d'un événement critique en fonction du comportement de sous-systèmes particuliers (les systèmes d'intervention d'urgence, par exemple).

Si elle est quantifiée, l'analyse causes-conséquences donne une estimation de la probabilité des différentes conséquences possibles à la suite d'un événement critique.

Dans la mesure où chaque séquence dans un diagramme causes-conséquences est une combinaison de sous-arbres de pannes, l'analyse causes-conséquences peut être utilisée pour élaborer des arbres de pannes de grande taille.

Puisque la génération et l'utilisation des diagrammes sont complexes, cette technique a tendance à être appliquée lorsque l'amplitude des conséquences potentielles de défaillance justifie un effort important.



IEC

Figure B.4 – Exemple de diagramme causes-conséquences

B.5.5.3 Entrées

Une bonne compréhension du système, ainsi que de ses modes et scénarios de défaillance, est nécessaire.

B.5.5.4 Résultats

Les résultats de l'ACC sont les suivants:

- une représentation graphique du déroulement d'une défaillance potentielle d'un système, et montrant les causes et les conséquences;
- une estimation de la probabilité d'occurrence de chaque conséquence potentielle, en fonction de l'analyse des probabilités d'occurrence de conditions particulières à la suite d'un événement critique.

B.5.5.5 Avantages et limites

En plus des avantages des arbres de pannes et d'événements, l'ACC est plus à même de représenter simultanément les causes et les conséquences d'un événement d'intérêt, ainsi que les dépendances temporelles, que ces autres techniques.

L'ACC présente toutefois l'inconvénient d'être plus complexe que les arbres de pannes et d'événements, en ce qui concerne la conception et dans la manière de traiter les dépendances lors de la quantification.

B.5.5.6 Documents de référence

- [47] ANDREWS J.D, RIDLEY L.M. 2002. *Application of the cause consequence diagram method to static systems*
- [48] NIELSEN D.S. *The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis*

B.5.6 Analyse par arbre d'événement (AAE)

B.5.6.1 Vue d'ensemble

L'AAE est une technique graphique qui représente les séquences mutuellement exclusives des événements qui pourraient survenir à la suite d'un événement initiateur, selon le fonctionnement ou non des différents systèmes conçus pour en faire varier les conséquences. L'arbre peut être quantifié afin de donner les probabilités des différents résultats possibles (voir Figure B.5).

L'arbre commence par l'événement initiateur, puis des lignes sont tracées pour représenter la réussite ou la défaillance de chaque moyen de maîtrise. La probabilité de défaillance ou de réussite peut être assignée à chaque moyen de maîtrise, à partir du jugement de l'expert, des données ou d'analyses par arbre de panne individuelles. Les probabilités sont des probabilités conditionnelles. Par exemple, la probabilité pour qu'un élément fonctionne n'est pas la probabilité obtenue à partir des essais en conditions normales, mais la probabilité pour qu'il fonctionne dans les conditions de l'événement initiateur.

La fréquence des différents résultats est représentée par le produit des probabilités conditionnelles individuelles et de la probabilité ou fréquence de l'événement initiateur, étant donné que les différents événements sont indépendants. La Figure B.5 prend pour hypothèse une probabilité de déclenchement de l'événement égale à 1.

B.5.6.2 Utilisation

L'AAE peut être utilisée de manière qualitative pour aider à analyser les scénarios et les séquences d'événements possibles après un événement initiateur, afin d'explorer comment les résultats sont affectés par les différents moyens de maîtrise. Elle peut être appliquée à tous les niveaux d'une organisation et à tous les types d'événements initiateurs.

L'AAE quantitative peut être utilisée pour étudier l'acceptabilité des moyens de maîtrise et l'importance relative de différents moyens de maîtrise pour le niveau de risque global. L'analyse quantitative nécessite que les moyens de maîtrise fonctionnent ou non (autrement dit elle ne peut pas tenir compte des moyens de maîtrise dégradés) et que les moyens de maîtrise soient indépendants. Tel est principalement le cas pour les problèmes opérationnels. L'AAE peut être utilisée pour modéliser les événements initiateurs à l'origine de pertes ou de gains. Toutefois, les circonstances de recherche des vecteurs d'optimisation des gains sont plus souvent modélisées dans un arbre de décision (B.9.3).

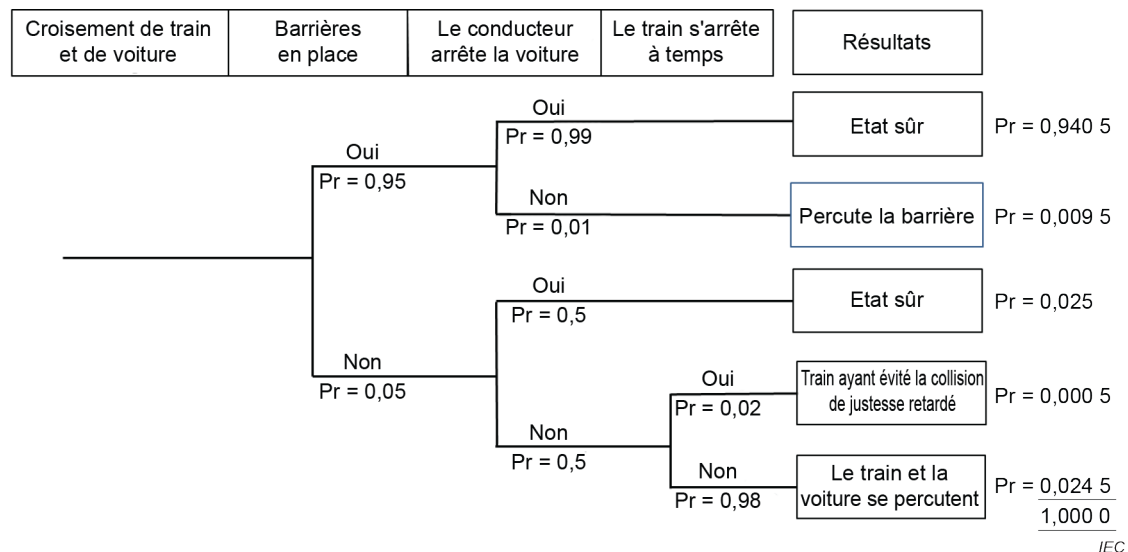


Figure B.5 – Exemple d'analyse par arbre d'événement

B.5.6.3 Entrées

Les entrées sont les suivantes:

- un événement initiateur spécifique;
- les informations concernant les barrières et les moyens de maîtrise et, pour l'analyse quantitative, les probabilités de défaillance;
- une compréhension des scénarios possibles.

B.5.6.4 Résultats

Les résultats de l'analyse par arbre d'événement sont les suivants:

- descriptions qualitatives des résultats possibles découlant des événements initiateurs;
- estimations quantitatives des taux/fréquences ou probabilités des événements et importance relative des différentes séquences de défaillance et des événements contributifs;
- évaluations quantitatives de l'efficacité des moyens de maîtrise.

B.5.6.5 Avantages et limites

Les avantages de l'analyse par arbre d'événement incluent ce qui suit.

- Les scénarios possibles après un événement initiateur sont analysés et l'influence de la réussite ou de la défaillance des moyens de maîtrise est montrée clairement dans un diagramme qui peut être quantifié, si besoin.
- Elle identifie des événements finaux qui pourraient autrement rester imprévus.
- Elle identifie les potentielles défaillances localisées, les zones de vulnérabilité du système et les contre-mesures peu avantageuses, et peut donc être utilisée pour améliorer l'efficacité des moyens de maîtrise.
- Elle tient compte de la temporalité et des effets domino qui gênent la modélisation sous forme d'arbres de pannes.

Les limites incluent ce qui suit.

- Pour que l'analyse soit exhaustive, il est nécessaire d'identifier tous les événements initiateurs possibles. Il existe toujours un risque d'oublier certains événements initiateurs importants ou certaines séquences d'événements.

- Seuls les états de réussite et de défaillance d'un système sont traités, et il est difficile d'y intégrer des moyens de maîtrise qui fonctionnent partiellement, des réussites à retardement ou des événements de remise en état.
- Tous les vecteurs sont conditionnels pour les événements se produisant sur des nœuds précédents le long du vecteur. La plupart des dépendances le long des vecteurs possibles sont donc résolues. Toutefois, certaines dépendances (comme les composants, les systèmes utilitaires et les opérateurs) pourraient être ignorées, ce qui donnerait lieu à des estimations optimistes de la vraisemblance de certaines conséquences particulières.
- Pour les systèmes complexes, l'arbre d'événement peut être difficile à créer de toutes pièces.

B.5.6.6 Documents de référence

- [49] IEC 62502, *Techniques d'analyse de la sûreté de fonctionnement – Analyse par arbre d'événement (AAE)*
- [50] IEC TR 63039, *Probabilistic risk analysis of technological systems – Estimation of final event rate at a given initial state* (disponible en anglais seulement)

B.5.7 Analyse par arbre de panne (AAP)

B.5.7.1 Vue d'ensemble

La technique AAP permet d'identifier et d'analyser les facteurs qui contribuent à un événement non souhaitable spécifié (appelé "événement de tête"). L'événement de tête est analysé d'abord en identifiant ses causes immédiates et nécessaires. Il peut s'agir de défaillances matérielles ou logicielles, d'erreurs humaines ou de tout autre événement pertinent. La relation logique entre ces causes est représentée par un certain nombre de portes comme ET et OU. Chaque cause est ensuite analysée de manière séquentielle en utilisant la même méthode jusqu'à ce qu'une nouvelle analyse devienne improductive. Le résultat est représenté de manière graphique sous la forme d'une arborescence (voir Figure B.6), qui est la représentation graphique d'une équation booléenne.

B.5.7.2 Utilisation

L'AAP est utilisée principalement au niveau opérationnel et pour les problèmes à court ou moyen terme. Elle est utilisée de manière qualitative pour identifier les causes et les vecteurs possibles qui mènent à l'événement de tête, ou de manière quantitative pour calculer la probabilité de l'événement de tête. Une logique stricte doit être suivie pour l'analyse quantitative. C'est-à-dire que les événements saisis en entrée des portes ET doivent être à la fois nécessaires et suffisants pour causer l'événement au-dessus d'eux, et que les événements des portes OU représentent toutes les causes possibles de l'événement au-dessus d'eux, chacun d'entre eux pouvant en être la seule cause. Les techniques qui s'appuient sur des diagrammes de décision binaires ou sur l'algèbre booléenne sont ensuite utilisées pour représenter les modes de défaillance en double.

L'AAP peut être utilisée pendant la conception pour choisir entre différentes options, ou pendant les opérations pour identifier comment les défaillances majeures peuvent se produire, ainsi que l'importance relative des différents vecteurs qui mènent à l'événement de tête.

L'arbre des causes, utilisé rétrospectivement pour analyser les événements qui se sont déjà produits, et l'arbre de réussite, où l'événement de tête est une réussite, sont des techniques très proches. La dernière est utilisée pour étudier les causes d'une réussite, afin d'obtenir d'autres réussites ultérieures.

Les probabilités ont tendance à être plus élevées dans un arbre de réussite que dans un arbre de panne et, lors du calcul de la probabilité de l'événement de tête, il convient de tenir compte de la possibilité que les événements ne soient pas mutuellement exclusifs.

B.5.7.3 Entrées

Les entrées pour l'analyse par arbre de panne sont les suivantes.

- Une bonne compréhension du système et des causes de la défaillance ou de la réussite est exigée, ainsi qu'une compréhension technique de la manière dont le système se comporte dans différentes circonstances. Des diagrammes détaillés sont utiles pour faciliter l'analyse.
- Pour tous les événements de base, l'analyse quantitative d'un arbre de panne exige des données sur les taux de défaillances, la probabilité d'un état de panne ou la fréquence des pannes et, le cas échéant, les taux de réparation/remise en état, etc.
- Pour les situations complexes, un logiciel est recommandé, ainsi qu'une compréhension de la théorie des probabilités et de l'algèbre booléenne afin que les entrées soient saisies correctement dans le logiciel.

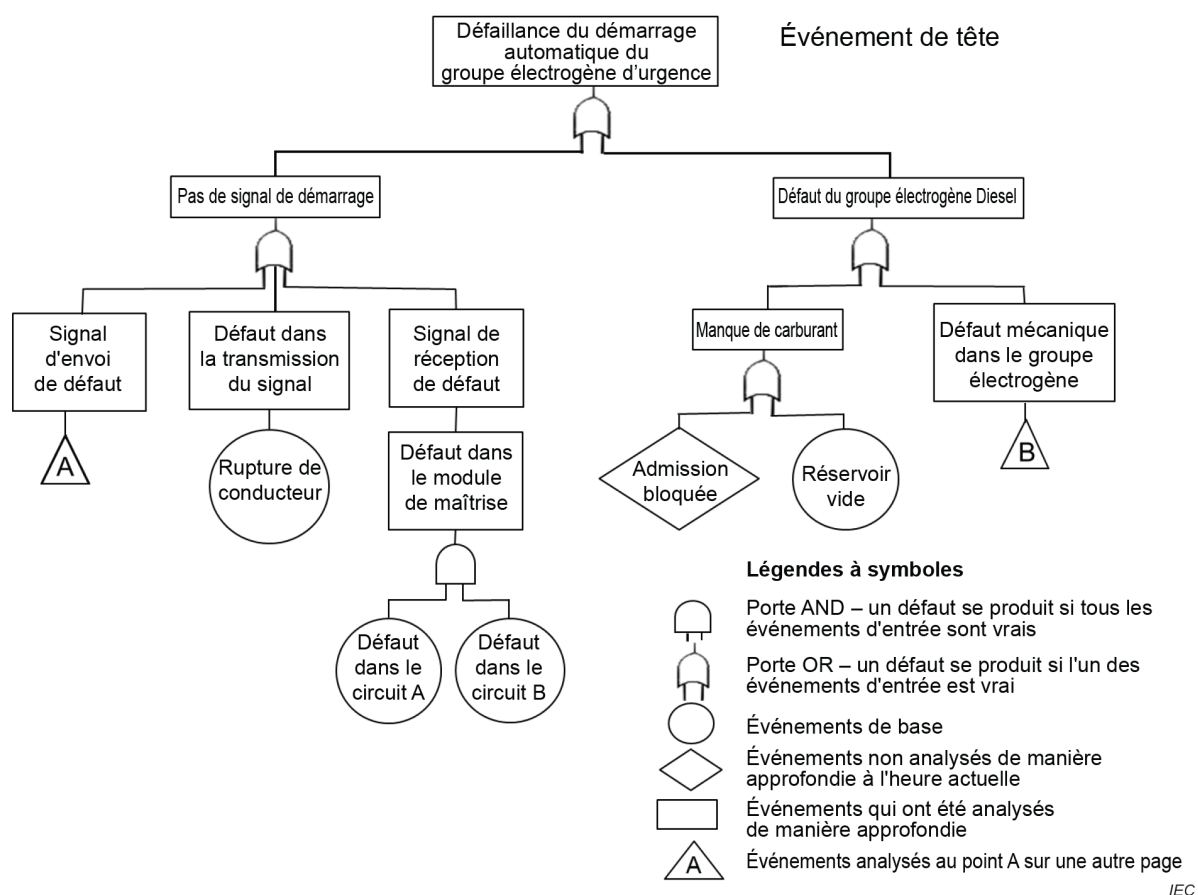


Figure B.6 – Exemple d'arbre de panne

B.5.7.4 Résultats

Les résultats de l'analyse par arbre de panne sont les suivants:

- une représentation graphique du déroulement de l'événement de tête, présentant les vecteurs d'interaction, dont chacun provoque la survenue de deux événements (de base) ou plus;
- une liste des coupes minimales (vecteurs individuels vers la défaillance) avec, si les données sont disponibles, la probabilité de survenue de chacune d'elles;
- dans le cas de l'analyse quantitative, la probabilité de l'événement de tête et l'importance relative des événements de base.

B.5.7.5 Avantages et limites

Les avantages de l'analyse par arbre de panne incluent ce qui suit.

- Elle constitue une approche disciplinée et hautement systématique, mais également suffisamment souple pour permettre d'analyser différents facteurs, y compris les interactions humaines et les phénomènes physiques.
- Elle est particulièrement utile à l'analyse de systèmes disposant de nombreuses interfaces et interactions.
- Elle fournit une représentation graphique qui conduit à une meilleure compréhension du comportement du système et des facteurs impliqués.
- L'analyse logique des arbres de pannes et la définition des coupes sont utiles pour identifier les vecteurs de défaillance simples dans un système très complexe, dans lequel des combinaisons particulières d'événements et de séquences d'événements donnant lieu à l'événement de tête pourraient être ignorées.
- Elle peut s'adapter aux problèmes simples ou complexes avec un niveau d'effort qui dépend de la complexité.

Les limites incluent ce qui suit.

- Dans certains cas, il peut être difficile d'établir que tous les vecteurs importants menant vers l'événement de tête sont inclus; par exemple, inclure toutes les sources d'allumage dans l'analyse d'un incendie. Dans ces cas, il n'est pas possible de calculer la probabilité de l'événement de tête.
- Les interdépendances temporelles ne sont pas traitées.
- L'AAP traite seulement les états binaires (réussite/défaillance).
- Les erreurs humaines peuvent être intégrées dans un arbre de panne, mais la nature et l'étendue de ces défaillances peuvent être difficiles à définir.
- L'AAP analyse un seul élément de tête. Elle n'analyse pas les défaillances secondaires ou accessoires.
- Une AAP peut devenir très volumineuse pour les systèmes à grande échelle.

B.5.7.6 Documents de référence

[51] IEC 61025, *Analyse par arbre de panne (AAP)*

[16] IEC 62740, *Analyse de cause initiale (RCA)*

B.5.8 Analyse de fiabilité humaine (AFH)

B.5.8.1 Vue d'ensemble

L'AFH désigne un groupe de techniques qui vise à évaluer la contribution d'un individu à la fiabilité et à la sûreté d'un système en identifiant et en analysant son potentiel d'actions incorrectes. Bien qu'elle soit le plus souvent appliquée aux performances dégradées des opérateurs dans le contexte de la sécurité, des méthodes semblables peuvent s'appliquer aux niveaux de performances améliorés. L'AFH s'applique au niveau tactique, à des tâches spécifiques pour lesquelles il est essentiel que les performances soient correctes.

D'abord, une analyse hiérarchique des tâches identifie les étapes et les sous-étapes d'une activité donnée. Les mécanismes d'erreur potentiels sont identifiés pour chaque sous-étape, souvent à l'aide d'un ensemble d'invites sous forme de mots clés (par exemple, trop tôt, trop tard, objet incorrect, action incorrecte, objet correct).

Les sources de ces erreurs (distraction, délai imparti trop court, etc.) peuvent être identifiées, et ces informations peuvent être utilisées pour réduire la vraisemblance d'erreur dans cette tâche. Les facteurs inhérents à l'individu lui-même, à l'organisation ou à l'environnement et qui influencent la probabilité d'erreur (facteurs de performance, FP) sont également identifiés.

La probabilité d'une action incorrecte peut être estimée par différentes méthodes, y compris en utilisant une base de données des tâches semblables ou le jugement d'un expert. Habituellement, un taux d'erreur nominal pour un type de tâche est défini, puis un multiplicateur est appliqué pour représenter les facteurs comportementaux ou environnementaux qui augmentent ou réduisent la probabilité de défaillance. Différentes méthodes ont été mises au point pour appliquer ces étapes de base.

Les premières méthodes mettaient beaucoup l'accent sur l'estimation de la vraisemblance de défaillance. Les méthodes qualitatives récentes se concentrent sur les causes cognitives des variations des performances humaines, avec une analyse qui porte davantage sur la manière dont les performances sont modifiées par les facteurs externes, et moins sur les tentatives de calcul des probabilités de défaillance.

B.5.8.2 Utilisation

L'AFH qualitative peut être utilisée:

- pendant la conception, pour que les systèmes soient conçus de manière à réduire le plus possible les probabilités d'erreur des opérateurs;
- pendant une modification du système pour vérifier si les performances humaines sont susceptibles d'être influencées dans un sens ou dans l'autre;
- pour améliorer les procédures afin de réduire les erreurs;
- pour aider à identifier et à réduire les facteurs d'erreur au sein des arrangements environnementaux ou organisationnels.

L'AFH quantitative est utilisée pour fournir des données sur les performances humaines qui serviront d'entrées pour les méthodes par arbre logique ou pour d'autres techniques d'appréciation du risque.

B.5.8.3 Entrées

Les entrées sont les suivantes:

- informations permettant de définir les tâches qu'il convient que les personnes réalisent;
- expérience concernant les types d'erreurs ou de performances extraordinaires qui surviennent en pratique;
- expertise concernant les performances humaines et les facteurs qui les influencent;
- expertise concernant la ou les technique(s) à utiliser.

B.5.8.4 Résultats

Les résultats comprennent:

- une liste d'erreurs ou de performances extraordinaires qui peuvent se produire et des méthodes permettant de les améliorer en reprenant la conception du système;
- les modes de performances humaines, leurs types, leurs causes et leurs conséquences;
- une appréciation qualitative ou quantitative du risque posé par les différences de performances.

B.5.8.5 Avantages et limites

Les avantages de l'analyse de fiabilité humaine incluent ce qui suit.

- Elle propose un mécanisme formel permettant d'inclure les performances humaines dans la prise en compte des risques liés aux systèmes dans lesquels l'intervention humaine joue un rôle prépondérant.

- La prise en compte formelle des modes et des mécanismes des performances humaines, à partir d'une compréhension des mécanismes cognitifs, peut aider à identifier des moyens de modifier les risques.

Les limites incluent ce qui suit.

- Ces méthodes sont mieux adaptées aux tâches routinières effectuées dans des environnements bien maîtrisés. Elles sont moins utiles pour les tâches complexes ou lorsque les actions doivent s'appuyer sur des sources d'informations multiples et potentiellement contradictoires.
- De nombreuses activités ne disposent pas de mode réussite/échec simple. L'AFH a du mal à traiter les impacts partiels sur les performances comme la qualité des actions ou des décisions.
- La quantification a tendance à dépendre largement de l'opinion d'expert, car très peu de données vérifiées sont disponibles.

B.5.8.6 Documents de référence

- [51] IEC 62508, *Lignes directrices relatives aux facteurs humains dans la sûreté de fonctionnement*
- [52] BELL Julie, HOLROYD Justin, *Review of human reliability assessment method*
- [53] OCDE, *Establishing the Appropriate Attributes in Current Human Reliability Assessment Techniques for Nuclear Safety*

B.5.9 Analyse de Markov

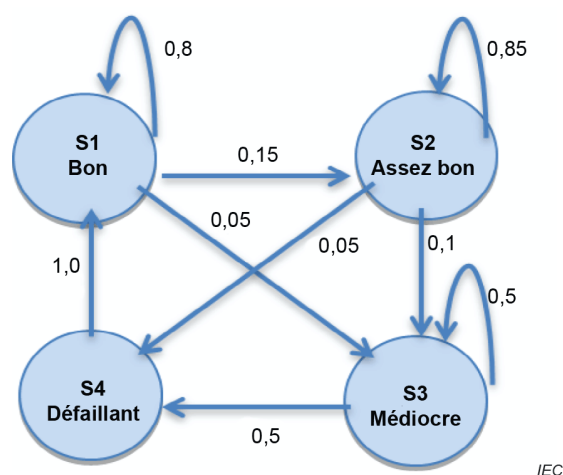
B.5.9.1 Vue d'ensemble

L'analyse de Markov est une technique quantitative qui peut s'appliquer à tous les systèmes pouvant être décrits selon un ensemble d'états discrets et de transitions entre ces états, à condition que l'évolution par rapport à leur état en cours ne dépende pas de leur état à tout moment du passé.

L'hypothèse habituelle est que les transitions entre les états ont lieu à des intervalles spécifiés, avec les probabilités de transition correspondantes (chaîne de Markov discrète). En pratique, cela se produit le plus souvent si le système est examiné à des intervalles réguliers pour déterminer son état. Dans certaines applications, les transitions sont gouvernées par des périodes aléatoires réparties de façon exponentielle avec les taux de transition correspondants (chaîne de Markov à temps continu). Cette chaîne est couramment utilisée pour les analyses de la sûreté de fonctionnement, voir IEC 61165.

Les états et leurs transitions peuvent être représentés dans un diagramme de Markov, comme à la Figure B.7. Ici, les cercles représentent les états et les flèches représentent les transitions entre les états et les probabilités de transitions correspondantes. Cet exemple comporte seulement quatre états: bon (S1), assez bon (S2), médiocre (S3) et défaillant (S4). L'hypothèse retenue est que le système est inspecté chaque matin et classé dans l'un de ces quatre états. Si le système est défaillant, il est toujours réparé le jour même et remis à l'état "bon".

Le système peut également être représenté par une matrice de transition, comme dans le Tableau B.4. Noter que dans ce tableau, la somme de chaque ligne est 1, étant donné que les valeurs représentent les probabilités de toutes les transitions possibles dans chaque cas.



IEC

Figure B.7 – Exemple de diagramme de Markov

Tableau B.4 – Exemple de matrice de Markov

		Etat suivant la transition			
		S1, Bon	S2, Assez bon	S3, Médiocre	S4, Défaillant
Etat actuel	S1, Bon	0,8	0,15	0,05	0
	S2, Assez bon	0	0,85	0,1	0,05
	S3, Médiocre	0	0	0,5	0,5
	S4, Défaillant	1	0	0	0

B.5.9.2 Utilisation

L'analyse de Markov peut être utilisée pour évaluer:

- la probabilité à long terme qu'un système se trouve dans un état spécifié; par exemple, il pourrait s'agir des chances qu'une machine fonctionne comme exigé, qu'un composant soit défaillant ou qu'un niveau d'approvisionnement tombe sous un seuil critique;
- le moment attendu pour la première défaillance d'un système complexe (temps de premier passage), ou la durée attendue avant qu'un système retourne à un état spécifié (temps de retour).

Le Tableau B.5 donne des exemples de systèmes, d'états et de transitions dans différents domaines.

Tableau B.5 – Exemples de systèmes auxquels l'analyse de Markov peut s'appliquer

Systèmes	Etats	Transitions
Systèmes techniques	Etat des machines	Détérioration, panne, réparation
Production	Niveau de production	Exploitation, nettoyage, redémarrage
Marketing	Achat de marque	Fidélité à une marque, changement de marque
Comptabilité	Etat des comptes débiteurs	Paieement, amortissement, extension
Soins médicaux	Etat des patients	Infection, rémission, traitement, récédive
Réservoir	Quantité d'eau	Débit entrant, débit sortant, évaporation
Ressources humaines	Catégories d'emplois	Mouvements d'une catégorie d'emplois à une autre

B.5.9.3 Entrées

Dans une analyse de Markov, les entrées sont un ensemble d'états discrets où le système peut se trouver, une compréhension de toutes les transitions possibles qu'il est nécessaire de modéliser et des estimations des probabilités de transition ou des taux de transition (dans le cas d'une chaîne de Markov à temps continu CTMC).

B.5.9.4 Résultats

L'analyse de Markov génère des estimations de la probabilité qu'un système se trouve dans un état donné. Elle vient à l'appui de nombreuses décisions concernant le type d'interventions qu'un responsable pourrait entreprendre dans un système complexe (par exemple, pour faire varier les états du système et les transitions entre ces états).

B.5.9.5 Avantages et limites

Les avantages de l'analyse de Markov incluent ce qui suit.

- Elle peut être utilisée pour modéliser des systèmes dynamiques à états multiples.
- Les diagrammes de transition d'état fournissent des structures simples et faciles à communiquer.

Les limites incluent ce qui suit.

- Les hypothèses pourraient ne pas s'appliquer à tous les systèmes considérés; en particulier les probabilités de transition ou les taux de transmission entre les états peuvent varier au fil du temps selon la détérioration et l'adaptation du système.
- Une modélisation fidèle peut exiger qu'un grand nombre de données soient rassemblées et validées.
- Si le nombre de données est trop élevé, la réponse est réduite à une moyenne.

B.5.9.6 Documents de référence

[54] IEC 61165, *Application des techniques de Markov*

[55] OXLEY, ALAN. *Markov Processes in Management Science*

B.5.10 Simulation de Monte-Carlo

B.5.10.1 Vue d'ensemble

Certains calculs réalisés pendant l'analyse de risques impliquent des distributions. Toutefois, il n'est pas facile de réaliser des calculs comprenant des distributions, car souvent, les

solutions analytiques ne sont pas déductibles à moins que la forme des distributions soit bien spécifiée, et seulement avec des restrictions et des hypothèses qui pourraient ne pas être réalistes. Dans ces circonstances, les techniques comme la simulation de Monte-Carlo fournissent un moyen d'entreprendre ces calculs et de développer les résultats. La simulation implique habituellement de prendre des valeurs d'échantillon aléatoires dans chacune des distributions de l'entrée, de faire des calculs pour déduire une valeur de résultat, puis de répéter le processus dans une série d'itérations afin de construire la distribution des résultats. Le résultat peut être donné sous la forme d'une simple distribution de probabilité ou de statistiques comme la valeur moyenne.

Les systèmes peuvent être développés à l'aide d'une feuille de calcul et d'autres outils conventionnels, mais des outils informatiques plus sophistiqués sont disponibles pour répondre aux exigences plus complexes.

B.5.10.2 Utilisation

D'une manière générale, la simulation de Monte-Carlo peut s'appliquer à tous les systèmes où:

- un ensemble d'entrées interagit pour définir un résultat;
- la relation entre les entrées et les résultats peut s'exprimer comme un ensemble de dépendances;
- les techniques analytiques ne sont pas en mesure de fournir des résultats pertinents ou lorsqu'il existe une incertitude dans les données d'entrée.

La simulation de Monte-Carlo peut être utilisée dans le cadre de l'appréciation du risque avec deux finalités distinctes:

- projection de l'incertitude sur des modèles d'analyse conventionnels;
- calculs probabilistes lorsque les techniques d'analyse ne s'appliquent pas ou ne sont pas réalisables.

Les applications incluent, entre autres, la modélisation et l'appréciation de l'incertitude des prévisions financières, des résultats en matière d'investissement, des prévisions liées au coût et à la planification du projet, des interruptions du processus métier et des exigences liées au recrutement.

B.5.10.3 Entrées

Les entrées de la simulation de Monte-Carlo sont les suivantes:

- un modèle de système qui retrace la relation entre différentes entrées, et entre les entrées et les résultats;
- des informations sur les types d'entrées ou sur les sources d'incertitudes qui doivent être représentées;
- la forme de résultat exigée.

Les données d'entrée liées à l'incertitude sont représentées comme des variables aléatoires dont les distributions sont plus ou moins réparties selon le niveau des incertitudes. Des distributions uniformes, triangulaires, normales et log-normales sont souvent utilisées à cette fin.

B.5.10.4 Résultats

Il peut s'agir d'une seule valeur, il peut être exprimé sous la forme d'une distribution des probabilités ou des fréquences, ou il peut s'agir de l'identification des principales fonctions du modèle dont l'impact sur le résultat est le plus important.

D'une manière générale, le résultat d'une simulation de Monte-Carlo est soit l'ensemble de la distribution des résultats, soit les mesures clés issues d'une distribution, comme:

- la probabilité d'un résultat défini;
- la valeur d'un résultat, dont les personnes concernées par le problème ont un certain niveau de confiance qu'elle ne sera pas dépassée. Par exemple, il peut s'agir d'un coût pour lequel les chances qu'il soit dépassé sont inférieures à 10 % ou d'une durée qui sera dépassée avec une certitude de 80 %.

Une analyse des relations entre les entrées et les résultats peut éclairer la signification relative de l'incertitude dans les valeurs d'entrée et identifier les cibles utiles susceptibles d'influencer l'incertitude du résultat.

B.5.10.5 Avantages et limites

Les avantages de l'analyse de Monte-Carlo incluent ce qui suit.

- En principe, la méthode peut concilier toutes les distributions dans une variable d'entrée, y compris les données empiriques déduites des observations de systèmes connexes.
- Les modèles sont relativement simples à développer et peuvent être étendus à mesure de l'évolution des besoins.
- Toutes les influences ou relations peuvent être représentées, y compris les effets tels que les dépendances conditionnelles.
- L'analyse de sensibilité peut être appliquée pour distinguer les influences importantes de celles qui le sont moins.
- Les modèles peuvent être aisément compris étant donné que la relation entre les entrées et les résultats est transparente.
- Elle fournit une mesure de l'exactitude d'un résultat.
- Des logiciels sont facilement disponibles.

Les limites incluent ce qui suit.

- L'exactitude des solutions dépend du nombre de simulations pouvant être réalisées.
- L'utilisation de cette technique repose sur l'aptitude à représenter les incertitudes liées aux paramètres par une distribution valide.
- Il peut être difficile de créer un modèle qui représente adéquatement la situation.
- Des modèles volumineux et complexes peuvent faire concurrence au programme de modélisation et rendre le début du processus difficile pour les différentes parties prenantes.
- Cette technique a tendance à réduire le plus possible les risques de type "conséquences élevées/faible probabilité".

L'analyse de Monte-Carlo évite de donner trop de poids aux résultats improbables aux conséquences élevées, en reconnaissant que tous ces résultats ont peu de chances de se produire simultanément au sein d'un ensemble de risques. Elle peut aussi avoir pour effet d'éliminer les événements extrêmes de la prise en compte, en particulier lorsque l'ensemble de risques pris en compte est étendu. Le décideur peut y puiser une confiance injustifiée.

B.5.10.6 Document de référence

- [56] Guide ISO/IEC 98-3:2008/Suppl 1: *Incertitude de mesure – Partie 3: Guide pour l'expression de l'incertitude de mesure (GUM: 1995) – Propagation de distributions par une méthode de Monte-Carlo*

B.5.11 Analyse d'impact sur la vie privée (PIA) / analyse d'impact sur la protection des données (DPIA)

B.5.11.1 Vue d'ensemble

Les méthodes d'analyse d'impact sur la vie privée (PIA) (également appelée appréciation de l'impact sur la vie privée) et d'analyse d'impact sur la protection des données (DPIA) permettent d'analyser la manière dont les incidents et les événements pourraient avoir un impact sur la vie privée d'une personne, et d'identifier et de quantifier les aptitudes nécessaires à leur gestion. Le processus PIA/DPIA consiste à évaluer une proposition afin d'identifier les effets possibles sur la vie privée et les données personnelles d'une personne.

Les analyses PIA et DPIA permettent aux organisations d'identifier, d'évaluer et de traiter les risques pour la vie privée associés aux activités de traitement des données. Elles sont particulièrement importantes au moment de l'introduction d'un nouveau processus, système ou technologie de traitement des données. Les analyses PIA et DPIA font partie intégrante de l'adoption d'une approche de confidentialité intrinsèque.

Les DPIA aident également les organisations à satisfaire aux exigences des organismes de réglementation en matière de protection des données (par exemple, le Règlement général sur la protection des données (RGPD) de l'Union européenne) et à démontrer que les mesures appropriées ont été prises pour assurer cette conformité.

Le processus consiste plus spécifiquement à:

- analyser les conséquences potentielles d'une violation de la vie privée pour une personne physique (étude des risques de base);
- prendre en compte le fait qu'un traitement donné d'informations personnelles présente ou non un risque élevé en cas d'incident de confidentialité;
- effectuer une analyse approfondie des risques dans le cadre du traitement des données permettant d'identifier une personne.

Une PIA/DPIA peut être entreprise à l'aide de questionnaires, d'entretiens, d'ateliers structurés ou d'une combinaison de ces trois éléments, en s'appuyant sur les recommandations du Groupe de travail Article 29 et sur plusieurs modèles développés, par exemple, par l'ICO (Royaume-Uni), la CNIL (France) ou la NOREA (Pays-Bas).

B.5.11.2 Utilisation

Une PIA/DPIA est utilisée pour déterminer les conséquences de risques élevés sur les processus et les ressources associées (par exemple, les personnes, l'équipement et les technologies de l'information), afin de limiter les effets négatifs potentiels du traitement de l'information pour la vie privée des personnes.

Elle peut également être utilisée dans le cadre de l'analyse des conséquences, pour la prise en compte des conséquences du traitement de l'information d'une manière plus générale.

B.5.11.3 Entrées

Les entrées sont les suivantes:

- des informations concernant les objectifs, l'orientation stratégique, l'environnement, les actifs et les interdépendances de l'organisation;
- une appréciation des priorités d'après la précédente étude des risques de base;
- les caractéristiques des activités et opérations de l'organisation lors du traitement d'informations personnelles, y compris les processus, les ressources, les relations avec les autres organisations, les chaînes logistiques, les conventions d'externalisation et les différentes parties prenantes;

- des informations permettant d'apprécier les conséquences financières, légales et opérationnelles d'une fuite ou d'une perte d'informations personnelles sensibles (et plus particulièrement d'informations personnelles hautement sensibles);
- un questionnaire préparé ou tout autre moyen de rassembler des informations;
- les résultats des autres appréciations du risque et des analyses d'incidents critiques concernant les conséquences d'incidents pertinents (en particulier une fuite de données ou une perte de données, ainsi que tout autre incident impliquant la sécurité de l'information qui peut affecter le traitement prévu des données);
- la liste des personnes appartenant aux services pertinents de l'organisation et/ou des différentes parties prenantes à contacter.

B.5.11.4 Résultats

Les résultats comprennent:

- les documents qui décrivent les informations collectées comme entrées;
- une liste des processus d'informations critiques et des interdépendances associées, par ordre de priorité;
- un ensemble de scénarios présentant un risque élevé dans le cadre du traitement escompté des données à caractère personnel;
- les impacts documentés d'une fuite ou d'une perte d'informations personnelles sur une personne physique;
- les informations concernant les ressources et activités nécessaires pour limiter les conséquences potentielles sur les personnes concernées;
- la liste des produits et services concernés de l'organisation, par ordre de priorité;
- une appréciation des impacts dans le temps et de moyens de ne pas garantir la confidentialité, l'intégrité et la disponibilité des données personnelles (à haut risque), ainsi que des conséquences pour les personnes concernées;
- les durées d'interruption observées pour prendre des mesures de confinement et/ou de récupération des informations, et pour soumettre une déclaration aux autorités compétentes et, dans certains cas, à la ou aux personne(s) concernée(s).

B.5.11.5 Avantages et limites

Les avantages des méthodes PIA/DPIA incluent ce qui suit:

- une compréhension approfondie des processus critiques qui traitent des informations personnelles (sensibles) au sein de l'organisation ou en son nom;
- une appréciation de la mise en œuvre des principes de la confidentialité intrinsèque et par défaut;
- les informations nécessaires pour planifier la réponse d'une organisation en cas d'incident impliquant des données personnelles;
- la compréhension des principales ressources exigées en cas de fuite ou de perte de données personnelles;
- l'opportunité de redéfinir et revoir le traitement opérationnel des données personnelles par une organisation;
- dans le cas d'une obligation légale (par exemple, Règlement général européen sur la protection des données), une documentation visant à informer les autorités nationales avant le début d'une activité de traitement de données personnelles présentant un risque élevé.

Les limites incluent ce qui suit.

- Le calcul de la gravité potentielle d'un risque pour la vie privée d'une personne peut être simpliste ou sous-estimé pendant la phase initiale (étude des impacts sur la vie privée).

- La PIA/DPIA s'appuie sur les connaissances et les perceptions des participants qui remplissent les questionnaires, ou qui assistent aux entretiens ou ateliers.
- La dynamique de groupe et la pression des délais peut avoir un impact négatif sur l'analyse exhaustive d'un processus critique.
- Le niveau de compréhension adéquat des opérations et activités de l'organisation peut être difficile à obtenir lors du traitement de données personnelles.

B.5.11.6 Documents de référence

[57] UE: *Règlement général sur la protection des données* (Journal officiel de l'Union européenne, 4 mai 2016)

[58] ICO (Royaume-Uni): *Data protection impact assessments*

[59] CNIL (FR), *Privacy Impact Assessment (PIA)*

B.6 Techniques d'analyse des dépendances et des interactions

B.6.1 Cartographie causale

B.6.1.1 Vue d'ensemble

La cartographie causale capture les perceptions individuelles sous la forme de chaînes d'arguments dans un graphe orienté destiné à être examiné et analysé. Les événements, les causes et les conséquences peuvent être représentés sur la carte.

Habituellement, les cartes sont développées dans des ateliers où les participants provenant de différentes disciplines se voient attribuer les tâches de recueillir les informations, de les structurer et de les analyser. Les perceptions sont enrichies d'informations provenant de documents, si nécessaire. Les entrées peuvent être collectées à l'aide de différents outils allant des notes adhésives aux logiciels spécialisés d'aide à la prise de décision de groupe. Le dernier cas permet d'entrer directement les problèmes, ce qui peut représenter un moyen de travail hautement productif. Il convient que les outils choisis permettent de collecter les problèmes de manière anonyme afin de pouvoir créer un environnement ouvert et non conflictuel permettant de favoriser la discussion ciblée sur les relations de causalité.

D'une manière générale, le processus commence en générant des contributions qui ont un impact ou qui provoquent des événements liés au problème à l'étude. Elles sont ensuite regroupées selon leur contenu, puis explorées de manière à fournir une couverture complète.

Les participants examinent ensuite la manière dont chacun des événements pourrait avoir un impact sur les autres. Cela permet de relier les événements discrets entre eux pour former des parcours de raisonnement basés sur la causalité dans la carte. Le processus vise à favoriser le partage de connaissances concernant les événements incertains et à provoquer d'autres contributions par le biais du processus explicatif mis en place, ce qui est nécessaire pour construire les chaînes d'arguments qui décrivent comment un événement en affecte un autre. Il existe des règles claires concernant la collecte des nœuds qui représentent les événements et les relations, afin de garantir une modélisation fiable et complète.

Après l'élaboration du réseau d'événements dans le but de former une carte complète, il peut être analysé afin de déterminer les propriétés qui peuvent être utiles au management du risque: par exemple, pour définir les nœuds centraux qui correspondent aux événements dont la survenue est centrale et qui peuvent avoir des effets systémiques considérables; ou pour déterminer les boucles de rétroaction qui peuvent provoquer des comportements dynamiques et destructeurs.

B.6.1.2 Utilisation

La cartographie causale identifie les liens et les interactions entre les risques et les thèmes au sein d'une liste de risques.

Elle peut être utilisée rétrospectivement pour développer la carte causale d'un événement qui s'est produit (par exemple, un projet qui dépasse les délais et les budgets impartis, une défaillance d'un système). Les cartes causales rétrospectives peuvent révéler des déclencheurs, des conséquences et des dynamiques. Elles permettent de déterminer la causalité, ce qui pourrait être essentiel pour les réclamations.

Les cartes causales peuvent également s'utiliser de manière proactive pour obtenir une appréciation complète et systémique des scénarios d'événements. La carte peut ensuite être examinée pour permettre l'approfondissement des connaissances et pour servir de base à l'analyse quantitative des risques afin d'aider à définir les priorités.

Elles permettent de mettre au point un programme de traitement intégré plutôt que de prendre chaque risque en compte séparément.

Des ateliers d'analyse causale peuvent avoir lieu à intervalle régulier pour que la nature dynamique des risques soit appréciée et traitée de manière appropriée.

B.6.1.3 Entrées

Les données permettant d'orienter le développement des cartes causales peuvent provenir de différentes sources comme les entretiens individuels, où les cartes produites donnent une représentation circonstanciée de ce qui s'est produit ou pourrait se produire. Les données peuvent aussi être tirées de la documentation (rapports, documents constitutifs d'une réclamation, etc.). Ces données peuvent être exploitées directement ou être utilisées pour orienter le processus d'analyse des chaînes d'arguments liées aux événements par les participants à un atelier.

B.6.1.4 Résultats

Les résultats sont les suivants:

- les cartes causales qui fournissent une représentation graphique des événements liés au risque et des relations systémiques entre ces événements;
- les résultats d'une analyse des cartes causales utilisées pour identifier les groupes d'événements émergents, les événements critiques du fait de leur position centrale, les boucles de rétroaction, etc.;
- un document qui traduit les cartes en texte, qui rapporte les résultats clés et qui explique le choix des participants et du processus utilisé pour développer les cartes.

Il convient que les résultats fournissent des informations pertinentes pour les décisions relatives au management du risque, ainsi qu'un journal d'audit du processus utilisé pour générer ces informations.

B.6.1.5 Avantages et limites

Les avantages des cartes causales incluent ce qui suit.

- Les risques pertinents pour le problème considéré sont pris en compte selon les perspectives multiples des participants.
- La nature divergente et ouverte du processus permet d'explorer le risque en réduisant les chances de négliger des événements ou des relations critiques.
- Le processus permet de capturer efficacement les interactions entre les événements et de comprendre leurs relations.
- Le processus de détermination du réseau d'événements qui forme la carte peut construire le langage et la compréhension partagés qui sont essentiels à une gestion efficace du risque.

Les limites incluent ce qui suit.

- Le processus de cartographie n'est pas facile à apprendre, car il demande non seulement un savoir-faire en matière de cartographie, mais aussi l'aptitude à diriger des groupes tout en travaillant avec l'outil de cartographie;
- Les cartes sont de nature qualitative et lorsqu'une quantification est exigée, il est nécessaire que les cartes soient utilisées comme une entrée dans d'autres modèles appropriés.
- Le contenu de la carte est déterminé par les sources et il est donc essentiel de choisir soigneusement les participants, sans quoi des domaines cruciaux peuvent être oubliés.

B.6.1.6 Documents de référence

- [60] BRYSON, J. M., ACKERMANN, F., EDEN, C., & FINN, C. *Visible thinking unlocking causal mapping for practical business results*
- [61] ACKERMANN, F, HOWICK, S, QUIGLEY, J, WALLS, L, HOUGHTON, T. *Systemic risk elicitation: Using causal maps to engage stakeholders and build a comprehensive view of risks*

B.6.2 Analyse d'impacts croisés

B.6.2.1 Vue d'ensemble

L'analyse d'impacts croisés est le nom générique donné à une famille de techniques conçues pour évaluer les variations de la probabilité d'un ensemble d'événements donné, après la survenue de l'un d'entre eux.

L'analyse d'impacts croisés consiste à construire une matrice pour montrer l'interdépendance des différents événements. Les lignes donnent la liste de l'ensemble des événements ou des tendances qui pourraient se produire et les colonnes donnent les événements ou les tendances qui seraient potentiellement affectés par les événements des lignes. Ensuite, il est exigé que les experts estiment:

- la probabilité de chaque événement (indépendamment des autres) à un horizon temporel donné;
- la probabilité conditionnelle de chaque événement si chacun des autres événements se produit, c'est-à-dire que pour la paire d'événements i/j , les experts estiment
 - $P(i/j)$ – la probabilité de i si j se produit,
 - $P(i/\text{non } j)$ – la probabilité de i si j ne se produit pas.

Ces éléments sont entrés dans un ordinateur en vue de leur analyse.

Il existe plusieurs méthodes différentes de calcul des probabilités d'un événement en tenant compte de tous les autres événements. Quelle que soit la méthode utilisée, la procédure habituelle consiste à réaliser une simulation de Monte-Carlo où le modèle informatique choisit systématiquement des ensembles d'événements cohérents et répète l'opération un certain nombre de fois. À mesure que le nombre de répétitions augmente, une nouvelle probabilité a posteriori de survenue de chaque événement est générée.

Une analyse de sensibilité est réalisée en choisissant une estimation de la probabilité initiale ou une estimation de la probabilité conditionnelle pour laquelle il existe une incertitude. Ce jugement est modifié et la matrice est exécutée à nouveau.

B.6.2.2 Utilisation

L'analyse d'impacts croisés est utilisée pour les études de prévision et comme technique analytique pour prévoir comment différents facteurs influencent les décisions futures. Elle peut être combinée avec l'analyse de scénario (B.2.5) pour décider lesquels des scénarios produits sont les plus probables. Elle peut être utilisée lorsque les risques d'interaction sont multiples, par exemple, pour les projets complexes, ou pour gérer les risques pour la sécurité.

L'horizon temporel de l'analyse d'impacts croisés s'étend généralement du moyen au long terme; il peut s'étaler du présent à cinq ans ou jusqu'à 50 ans dans l'avenir. Il convient de mentionner l'horizon temporel de manière explicite.

La matrice des événements et leurs interdépendances peuvent être utiles pour les décideurs en tant que contexte général, même sans la probabilité calculée à partir de l'analyse.

B.6.2.3 Entrées

Cette méthode exige le recours à des experts qui connaissent bien les problèmes étudiés, qui ont la capacité d'envisager les futurs développements et qui sont capables d'estimer les probabilités de manière réaliste.

Des logiciels de soutien sont nécessaires pour calculer les probabilités conditionnelles. Cette technique exige une connaissance spécifique de la modélisation si l'utilisateur veut comprendre comment les données sont traitées par les logiciels. Le développement et l'exploitation des modèles nécessitent habituellement beaucoup de temps (plusieurs mois).

B.6.2.4 Résultat

Le résultat est une liste de tous les futurs scénarios possibles avec leur interprétation. Chaque exploitation du modèle produit un historique synthétique de l'avenir, ou un scénario, qui comprend la survenue de certains événements et la non-survenue des autres. D'après le modèle d'impacts croisés appliqué, les scénarios produits visent à générer le scénario le plus probable ou un ensemble de scénarios cohérents du point de vue statistique, ou bien un ou plusieurs scénarios possibles parmi l'ensemble complet.

B.6.2.5 Avantages et limites

Les avantages de l'analyse d'impacts croisés incluent ce qui suit.

- Il est relativement simple de mettre en œuvre un questionnaire d'impacts croisés.
- Elle attire l'attention sur les chaînes de causalité (*a* affecte *b*; *b* affecte *c*, etc.).
- Elle peut clarifier et améliorer les connaissances sur les futurs développements.
- Elle est utile pour explorer une hypothèse et pour trouver les points d'accord et de divergence.

Les limites incluent ce qui suit.

- Le nombre d'événements pouvant être inclus est limité en pratique par le logiciel et par le temps nécessaire aux experts. Le nombre d'exploitations exigé et le nombre de probabilités conditionnelles à estimer augmentent rapidement en même temps que le nombre d'événements inclus (par exemple, avec un ensemble de dix événements, un expert a besoin de fournir 90 jugements de probabilité conditionnelle).
- Une étude réaliste exige un travail considérable de la part des experts et le taux d'abandon observé est souvent élevé.
- Il est difficile de définir les événements à inclure et toute influence non comprise dans l'ensemble d'événements est entièrement exclue de l'étude; à l'inverse, l'inclusion d'événements non pertinents peut compliquer inutilement l'analyse finale des résultats.
- Comme pour d'autres techniques qui s'appuient sur le recours aux connaissances des experts, cette méthode repose sur le niveau d'expertise des personnes interrogées.

B.6.2.6 Document de référence

[62] CENTRE COMMUN DE RECHERCHE, COMMISSION EUROPÉENNE; *Cross impact analysis*; [consulté le 14 septembre 2017]

B.7 Techniques utilisées pour produire une mesure du risque

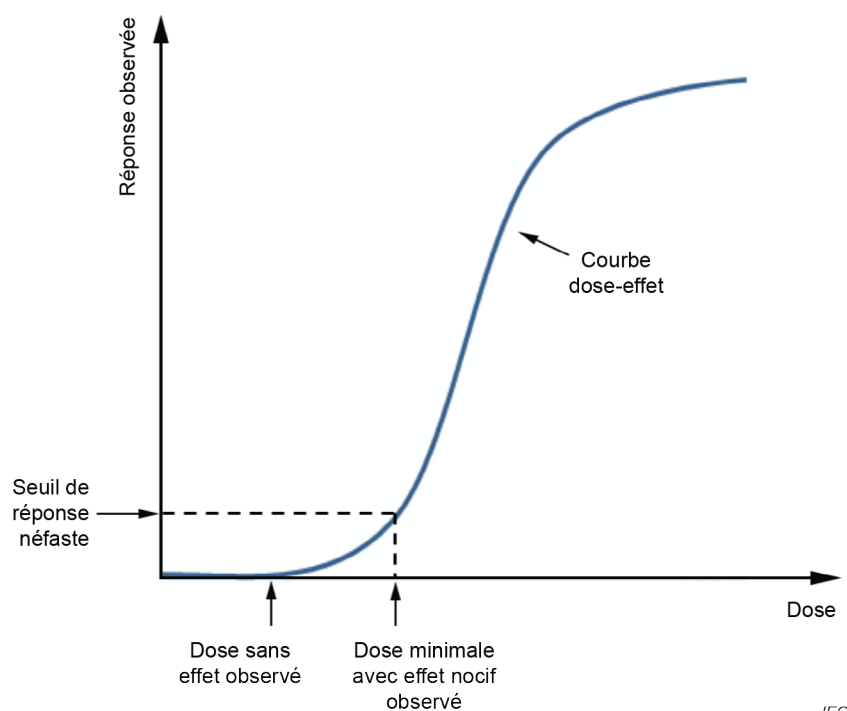
B.7.1 Appréciation du risque toxicologique

B.7.1.1 Vue d'ensemble

L'appréciation du risque dans le contexte des risques pour les végétaux, les animaux, les domaines écologiques et les êtres humains à la suite de leur exposition à une série de dangers environnementaux comprend les étapes suivantes.

Les risques pour les végétaux, les animaux, les domaines écologiques et les êtres humains peuvent être dus à des agents physiques, chimiques et/ou biologiques entraînant une altération de l'ADN, des malformations congénitales, une propagation de maladies, une contamination des chaînes alimentaires et une contamination de l'eau. L'appréciation de tels risques peut exiger l'application d'une diversité de techniques au cours des étapes suivantes.

- Formulation du problème: il s'agit de définir le contexte de l'appréciation en déterminant l'objectif de l'appréciation, l'étendue des populations ciblées et les types de dangers pris en compte.
- Identification et analyse des dangers: il s'agit d'identifier toutes les sources possibles de nuisance auxquelles est exposée la population ciblée dans le domaine d'application de l'étude et de comprendre la nature de ces dangers et comment ils interagissent avec la cible. Par exemple, en cas d'exposition d'une personne à un produit chimique, les conséquences envisagées peuvent inclure le risque de lésion de l'ADN, de cancer ou de malformations congénitales. En principe, l'identification et l'analyse des dangers reposent sur l'expertise et une revue de la documentation disponible.
- Evaluation dose-effet: les effets sur la population ciblée dépendent habituellement du niveau d'exposition ou de la dose. Des courbes dose-effet sont habituellement créées à partir d'essais sur les animaux, ou en s'appuyant sur des systèmes expérimentaux comme la culture des tissus. Pour les dangers liés aux micro-organismes ou aux espèces introduites, par exemple, la courbe dose-effet peut être déterminée à partir de données d'exploitation et d'études épidémiologiques. Le mécanisme produisant l'effet est déterminé dans la mesure du possible. La Figure B.8 montre une courbe dose-effet simplifiée.



IEC

Figure B.8 – Exemple de courbe dose-effet

- d) Appréciation de l'exposition: la dose qui sera reçue en pratique par la population ciblée est estimée. Cela implique souvent une analyse du cheminement, qui tient compte des différents vecteurs de propagation du danger, des barrières qui pourraient protéger la cible et des facteurs pouvant influencer le niveau d'exposition. Par exemple, en considérant un risque provenant d'une projection chimique: l'analyse d'exposition tiendrait compte de facteurs comme l'ampleur de la projection, les conditions de sa survenue, déterminerait si des personnes ou des animaux ont été directement exposés, la quantité de résidu déposée sur les végétaux, l'évolution dans l'environnement de tout pesticide infiltré dans le sol, s'il peut s'accumuler dans le corps des animaux, s'il se diffuse dans les nappes phréatiques, etc.
- e) Caractérisation du risque: les informations obtenues aux étapes précédentes sont rassemblées pour estimer la vraisemblance des conséquences particulières lorsque les effets de tous les vecteurs sont combinés.

B.7.1.2 Utilisation

Cette méthode fournit une mesure de l'amplitude du risque pour la santé humaine ou pour l'environnement. Elle est utilisée dans les énoncés des incidences environnementales pour indiquer si le risque lié à une exposition donnée est acceptable. Elle est également utilisée comme base pour définir les limites du risque acceptable.

B.7.1.3 Entrées

Les entrées sont les informations concernant les dangers toxicologiques, l'écosystème ciblé (y compris la santé humaine) et, dans la mesure du possible, les mécanismes impliqués. Habituellement, des mesures physiques sont exigées pour l'estimation des expositions.

B.7.1.4 Résultats

Le résultat est une estimation du risque pour la santé humaine ou écologique, exprimée de manière quantitative ou selon le mélange d'informations qualitatives et quantitatives fourni. Le résultat peut contenir les limites à utiliser pour définir les limites acceptables concernant le danger environnemental, comme la dose sans effet observé (voir Figure B.8).

B.7.1.5 Avantages et limites

Les avantages de cette forme d'analyse incluent ce qui suit.

- Elle permet de bien comprendre la nature du risque et les facteurs augmentant le risque.
- L'analyse des vecteurs est un outil très utile, adapté à tous les domaines de risque, pour identifier comment et dans quelle mesure il peut être possible d'améliorer les moyens de maîtrise ou d'en introduire de nouveaux.
- L'analyse peut servir de base à des règles simples concernant l'exposition acceptable, éligibles pour une application générale.

Les limites incluent ce qui suit.

- Elle exige d'obtenir les bonnes données, mais celles-ci ne sont peut-être pas immédiatement disponibles et d'importantes recherches pourraient donc être nécessaires.
- Son application nécessite un niveau élevé d'expertise.
- Un niveau élevé d'incertitude est souvent associé aux courbes dose-effet et aux modèles utilisés pour les créer.
- Lorsque la cible est écologique plutôt qu'humaine, et que le danger n'est pas chimique, les systèmes concernés pourraient être mal compris.

B.7.1.6 Documents de référence

[63] ORGANISATION MONDIALE DE LA SANTÉ, *Boîte à outils d'appréciation du risque pour la santé humaine: Dangers chimiques*

[64] US EPA, *Guidelines for ecological risk assessment*

B.7.2 Valeur en risque (VaR)

B.7.2.1 Vue d'ensemble

La valeur en risque (VaR) est couramment utilisée dans le secteur de la finance pour fournir un indicateur du montant de perte possible dans un portefeuille d'actifs financiers dans une période spécifique et jusqu'à un certain niveau de confiance. Les pertes supérieures à la VaR sont subies seulement avec une faible probabilité spécifiée.

La distribution des pertes et profits est habituellement déduite selon une méthode choisie parmi trois méthodes possibles.

- La simulation de Monte-Carlo (voir B.5.10) est utilisée pour modéliser les facteurs de variabilité dans le portefeuille et pour déduire la distribution. Cette approche est particulièrement utile, car elle fournit des informations sur les risques aux queues de distribution, et elle permet d'émettre des hypothèses de corrélations qui feront l'objet d'essais.
- Les modèles de simulation historique opèrent des projections en examinant rétrospectivement les résultats et les distributions observés. Cette approche est simple, mais elle peut être très trompeuse si les développements futurs ne correspondent pas à l'expérience passée, ce qui représente une limite importante en période de tensions sur le marché.
- Les méthodes analytiques s'appuient sur des hypothèses selon lesquelles les facteurs sous-jacents du marché ont une distribution normale multivariable. Avec cette méthode, les pertes et profits, qui ont aussi une distribution normale, peuvent être déterminés.

De nombreuses organisations financières utilisent une combinaison de ces approches.

Certains secteurs exigent que la VaR soit calculée sur la base de tensions sur le marché et de conditions de volatilité élevée, afin de fournir un ensemble crédible de résultats de type "scénario le plus défavorable".

Les mesures de la VaR sont couramment liées aux pertes à des horizons d'une journée et de deux semaines, avec des probabilités de pertes de 1 % et 5 %. Par convention, la VaR est exprimée sous la forme d'un nombre positif, bien qu'elle fasse référence à une perte.

Par exemple, la Figure B.9 montre la distribution de la valeur d'un portefeuille d'actifs financiers sur une période donnée, avec la distribution indiquée de manière cumulative. La Figure B.10 montre la zone où le portefeuille subit une perte, avec des valeurs de VaR de 1,6 million à 1 % (probabilité de perte de 0,01) et 0,28 million à 5 % (probabilité de perte de 0,05).

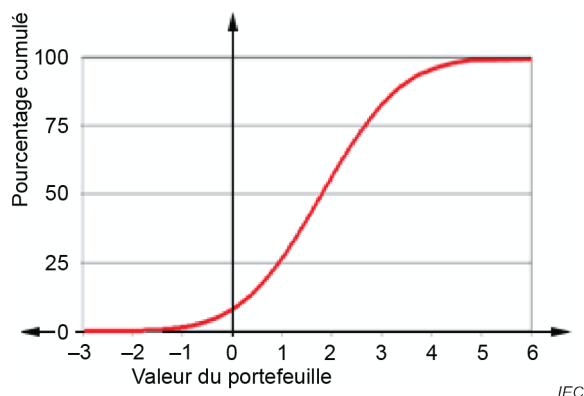


Figure B.9 – Distribution de la valeur

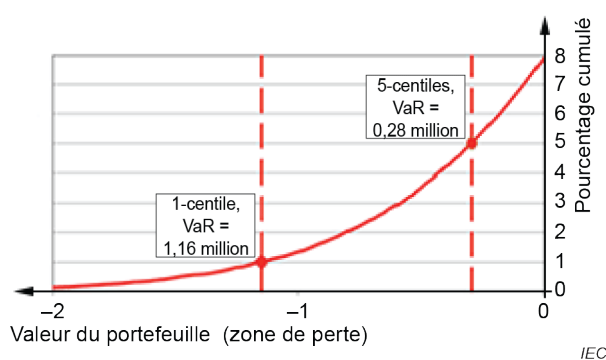


Figure B.10 – Détail des valeurs de la VaR dans la zone de pertes

B.7.2.2 Utilisation

La VaR se compose de trois paramètres: un montant des pertes possibles, la probabilité de ce montant de pertes et la période à laquelle la perte pourrait survenir. Elle est utilisée aux fins suivantes:

- pour fixer les limites à respecter par le gestionnaire de portefeuille concernant la perte maximale d'un portefeuille, en convenant d'une tolérance au risque ou d'un goût du risque;
- pour surveiller le "potentiel de risque" d'un portefeuille d'actifs à un moment donné, ainsi que les tendances concernant le "potentiel de risque";
- pour déterminer quelle part de capital économique, prudentiel ou réglementaire il peut être nécessaire de réserver pour un portefeuille spécifié;
- pour les déclarations aux organismes de réglementation.

B.7.2.3 Entrées

Les entrées sont les facteurs de marché qui affectent la valeur du portefeuille, par exemple les taux de change, les taux d'intérêt et les cours des actions. Habituellement, elles sont identifiées en décomposant les instruments du portefeuille en instruments plus simples liés directement aux facteurs de risque de base du marché, puis en interprétant les instruments réels comme des portefeuilles de ces instruments simplifiés. Les bailleurs de fonds et les organismes de réglementation peuvent exiger l'adoption de méthodes spécifiques pour apprécier les variables d'entrée.

B.7.2.4 Résultat

Sur une période donnée, la VaR calcule la perte potentielle d'un portefeuille d'actifs financiers pour une probabilité spécifiée. L'analyse peut également révéler la probabilité pour un montant de perte spécifié.

B.7.2.5 Avantages et limites

Les avantages incluent ce qui suit.

- Cette approche est directe et acceptée (ou exigée) par les organismes de réglementation financière.
- Elle peut être utilisée pour calculer les exigences relatives au capital économique, quotidiennement si nécessaire.

- Elle offre un moyen de fixer des limites pour un portefeuille boursier, conformément à un goût du risque convenu, et de surveiller les performances par rapport à ces limites, ce qui favorise la gouvernance.

Les limites incluent ce qui suit.

- La VaR est un indicateur et non une estimation spécifique de la perte possible. La perte maximale possible pour une situation donnée n'est pas clairement exprimée par un simple chiffre correspondant à la VaR avec une vraisemblance de perte de 1 % ou 5 % déduite de l'analyse de la VaR.
- La VaR présente plusieurs propriétés mathématiques non souhaitables. Par exemple, la VaR est une mesure de risque cohérente lorsqu'elle s'appuie sur une distribution elliptique comme la distribution normale habituelle, mais pas dans d'autres circonstances. A la queue de la distribution, les calculs sont souvent instables et peuvent s'appuyer sur des hypothèses spécifiques concernant les formes de distribution et les corrélations qui peuvent être difficiles à justifier, et qui pourraient ne pas perdurer en période de tensions sur le marché.
- Les modèles de simulation peuvent être complexes et prendre beaucoup de temps à appliquer.
- Les organisations peuvent avoir besoin de systèmes informatiques sophistiqués pour collecter les informations concernant le marché, sous une forme facile à utiliser et dans les délais, aux fins des calculs de la VaR.
- Il est nécessaire de prendre des valeurs d'hypothèse pour un ensemble de paramètres qui sont alors fixes dans le modèle. Si la situation varie et que ces hypothèses ne sont plus pertinentes, la méthode ne donnera pas de résultats raisonnables. Par conséquent, ce modèle de risque ne peut pas être utilisé en conditions d'instabilité.

B.7.2.6 Documents de référence

[65] CHANCE, D., BROOKS, R. (2010). *An introduction to derivatives and risk management*

[66] THOMAS J. and PEARSON Neil D. Value at risk. *Financial Analysts Journal* 2000 **56**, 47-67

B.7.3 Valeur en risque conditionnelle (CVaR) ou "expected shortfall" (ES)

B.7.3.1 Vue d'ensemble

La valeur en risque conditionnelle (CVaR), également appelée "expected shortfall" (ES), est une mesure de la perte attendue d'un portefeuille financier dans la tranche de a % des scénarios les plus défavorables. Cette mesure est très semblable à la VaR, mais est plus sensible à la forme de la queue inférieure (perte) de la distribution de valeur du portefeuille. La $CVaR(a)$ est la perte attendue selon les pertes qui ne surviennent que dans un certain pourcentage des cas. Par exemple, sur la Figure B.10, lorsque a vaut 5, alors la $CVaR(5)$ est la valeur attendue des pertes représentées par la courbe, à gauche de la ligne verticale qui traverse le repère des 5 %, c'est-à-dire la moyenne de toutes les pertes supérieures à 0,28 million.

B.7.3.2 Utilisation

Les techniques de calcul de la CVaR ont été appliquées à la mesure des risques de crédits, ce qui donne aux prêteurs un aperçu des variations du risque extrême dans tous les secteurs depuis le début de la crise financière. Figure B.11 montre le mieux la différence entre la CVaR et la VaR pour un portefeuille dans une situation de risque.

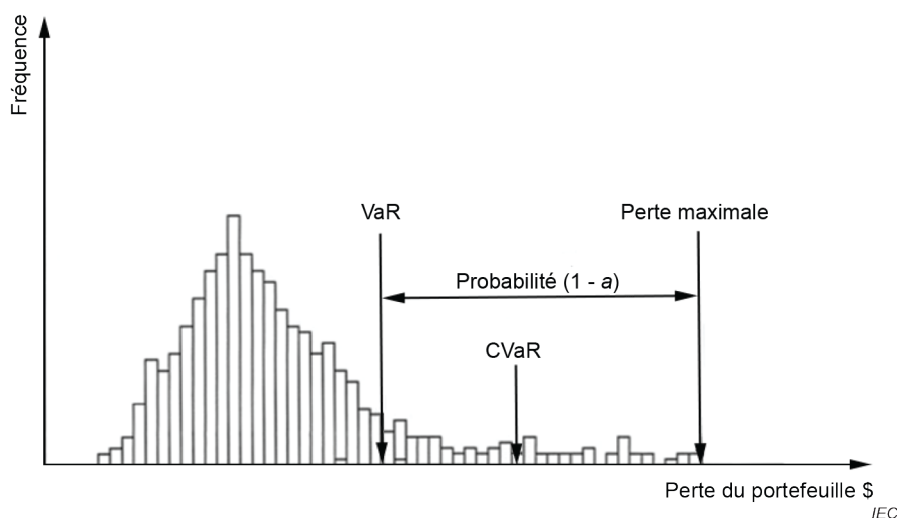


Figure B.11 – VaR et CVaR pour un portefeuille présentant une perte possible

B.7.3.3 Entrées et résultats

Voir la description de la valeur en risque (VaR) en B.7.2.

B.7.3.4 Avantages et limites

Les avantages incluent ce qui suit.

- La CVaR est plus sensible à la forme de la queue de distribution que la VaR.
- La CVaR évite certaines limites mathématiques inhérentes à la VaR.
- La CVaR est une mesure plus conservatrice que la VaR, car elle met l'accent sur les résultats à l'origine des plus grandes pertes.

Les limites incluent ce qui suit.

- La CVaR est un indicateur de perte potentielle, et non une estimation de la perte maximale possible.
- Comme pour la VaR, la CVaR est sensible aux hypothèses fondamentales concernant la volatilité de la valeur des actifs.
- La CVaR s'appuie sur des mathématiques complexes et exige une grande variété d'hypothèses.

B.7.3.5 Documents de référence

[67] CHOUDHRY, M. *An introduction to Value at Risk*

[68] *Value at Risk*. New York University. [consulté le 14 septembre 2017]. Disponible à l'adresse:
<http://people.stern.nyu.edu/adamodar/pdfiles/papers/VAR.pdf>

B.8 Techniques d'évaluation de l'importance d'un risque

B.8.1 Généralités

Les techniques traitées dans l'Article B.8 sont utilisées au sein d'un processus qui implique de décider si un risque doit être traité et de quelle manière le traiter. Certaines peuvent être utilisées pour décider si un risque particulier est tolérable ou acceptable, d'autres pour indiquer l'importance relative d'un risque ou pour classer les risques par ordre de priorité.

B.8.2 Critères ALARP et SFAIRP

B.8.2.1 Vue d'ensemble

ALARP et SFAIRP sont des acronymes qui contiennent le principe du "raisonnablement possible". Ils représentent les critères selon lesquels l'essai d'acceptabilité ou de tolérabilité d'un risque repose sur le fait qu'il soit possible, de manière raisonnable, d'agir pour réduire encore le risque. Le critère ALARP exige généralement que le niveau de risque soit réduit à un niveau aussi bas que raisonnablement possible (*as low as reasonably practicable*). Le critère SFAIRP exige généralement que la sécurité soit garantie dans la mesure où cela est raisonnablement possible (*so far as is reasonably practicable*). Le terme "raisonnablement possible" a été défini par la législation ou par la jurisprudence dans certains pays.

Les critères SFAIRP et ALARP visent à obtenir le même résultat, bien qu'ils divergent sur le point sémantique. ALARP garantit la sécurité en rendant le risque aussi faible que raisonnablement possible, tandis que SFAIRP ne fait aucune référence au niveau de risque. SFAIRP est habituellement interprété comme un critère permettant d'apprécier les moyens de maîtrise afin de déterminer si des traitements supplémentaires sont possibles; puis, lorsqu'ils sont possibles, s'ils sont réalisables. ALARP et SFAIRP font la part des choses pour arrêter les traitements du risque sur la base de coûts vraiment disproportionnés par rapport aux avantages gagnés, mais la mesure de cette possibilité dépend de la juridiction compétente. Par exemple, dans certaines juridictions, les études coûts-bénéfices (voir B.9.2) peuvent être utilisées pour étayer l'argument selon lequel le critère ALARP ou SFAIRP a été atteint.

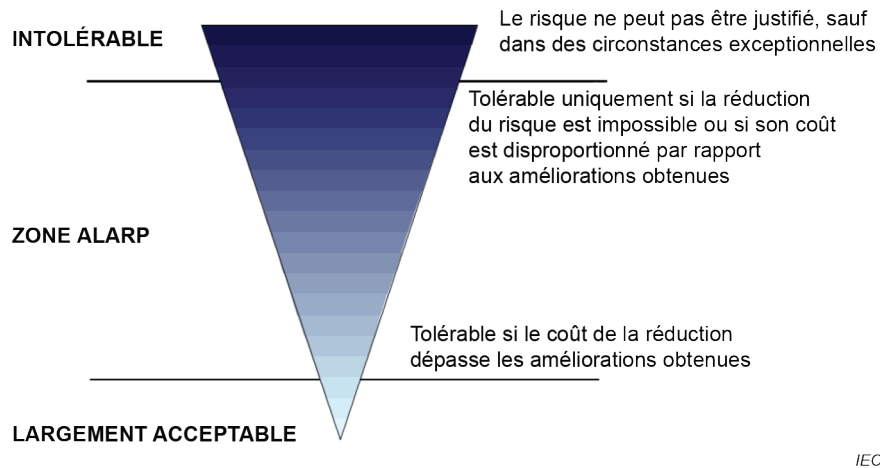
Le concept du critère ALARP, exprimé à l'origine par le Health and Safety Executive, au Royaume-Uni, est décrit à la Figure B.12. Dans certaines juridictions, des niveaux de risque quantifiés sont placés sur les limites entre les zones "intolérable", "ALARP" et "largement acceptable".

B.8.2.2 Utilisation

Les critères ALARP et SFAIRP sont utilisés pour décider si un risque nécessite d'être traité. Ils sont le plus souvent utilisés pour les risques liés à la sécurité et sont utilisés par les législateurs dans certaines juridictions.

Le modèle ALARP peut être utilisé pour classer les risques dans l'une des trois catégories suivantes:

- une catégorie de risque intolérable où le risque ne peut pas être justifié, sauf dans des circonstances exceptionnelles;
- une catégorie de risque largement acceptable où le risque est si faible qu'une réduction supplémentaire du risque peut ne pas être envisagée (mais pourrait être mise en œuvre si elle était réalisable et raisonnable);
- une zone intermédiaire entre ces limites (la zone ALARP) où il convient de mettre en œuvre une réduction supplémentaire du risque si cela est raisonnablement possible.



IEC

Figure B.12 – Diagramme ALARP

B.8.2.3 Entrées

Informations concernant:

- la source de risque et le risque associé;
- les critères relatifs aux limites de la zone ALARP;
- les moyens de maîtrise en place et les autres moyens de maîtrise possibles;
- les conséquences potentielles;
- la vraisemblance de ces conséquences;
- le coût des traitements possibles.

B.8.2.4 Résultat

Le résultat est une décision sur le fait qu'un traitement soit exigé et le traitement à appliquer.

B.8.2.5 Avantages et limites

Les avantages des critères ALARP/SFAIRP incluent ce qui suit.

- Ils fixent une norme commune de précautions, selon la jurisprudence et la législation, qui appuie le principe d'équité au sens où chaque individu a droit au même niveau de protection contre les risques, jugé par la loi, par opposition à une variable jugée tolérable ou acceptable par son organisation.
- Ils viennent à l'appui du principe d'utilité, car il convient que la réduction du risque n'exige pas davantage d'efforts que ce qui est raisonnablement possible.
- Ils permettent de fixer des objectifs de manière non prescriptive.
- Ils soutiennent l'amélioration continue vers l'objectif de la réduction des risques.
- Ils offrent une méthodologie transparente et objective pour examiner et définir les risques acceptables ou tolérables par le biais d'une concertation des parties prenantes.

Les limites incluent ce qui suit.

- L'interprétation du critère ALARP ou SFAIRP peut être difficile, car elle exige que les organisations comprennent le contexte législatif du raisonnablement possible et qu'elles exercent leur jugement vis-à-vis de ce contexte.
- L'application du critère ALARP ou SFAIRP aux nouvelles technologies peut être problématique, car les risques et les traitements possibles pourraient ne pas être connus ou bien compris.

- Les critères ALARP et SFAIRP fixent une norme commune de précautions que les organisations modestes peuvent ne pas pouvoir se permettre financièrement; ce qui peut les conduire à prendre des risques ou à cesser une activité.

B.8.2.6 Documents de référence

- [69] HSE, 2010a, *HID'S Approach To 'As Low As Reasonably Practicable' (ALARP) Decisions*
- [70] HSE, 2010b, *Guidance on (ALARP) decisions in control of major accident hazards (COMAH)*
- [71] HS, *Principles and guidelines to assist HSE in its judgments that duty-holders have reduced risk as low as reasonably practicable*

B.8.3 Diagrammes fréquence-nombre (F-N)

B.8.3.1 Vue d'ensemble

Un diagramme F-N est un type particulier de matrice conséquence/vraisemblance quantitative (B.10.3). Dans cette application, l'axe X représente le nombre cumulé de décès et l'axe Y la fréquence à laquelle ils se produisent. Les deux échelles sont logarithmiques pour s'adapter aux données usuelles. Les critères de risque sont généralement représentés sous forme de droites sur le graphique; plus la pente de la droite est importante, plus un nombre élevé de décès est évité par rapport à un nombre plus faible.

B.8.3.2 Utilisation

Les diagrammes F-N sont utilisés soit en tant qu'archives des résultats des incidents ayant impliqué la perte d'une vie humaine, soit pour afficher les résultats d'une analyse quantitative du risque de perte de vie par rapport à des critères d'acceptabilité prédéfinis.

La Figure B.13 montre deux exemples de critères désignés A et A-1, et B et B-1. Ils font la distinction entre une zone intolérable (au-dessus de A ou B), une zone largement acceptable (au-dessous de A-1 et B-1) et une zone entre les lignes où les risques sont acceptables s'ils sont aussi faibles que raisonnablement possible (ALARP) B.8.2). Les critères B présentent à la fois une pente plus importante (c'est-à-dire une tolérance plus faible aux décès multiples) et des limites globalement plus conservatrices. Six points se trouvent également sur la ligne C. Ils représentent les résultats d'une analyse quantitative du niveau de risque à comparer aux critères.

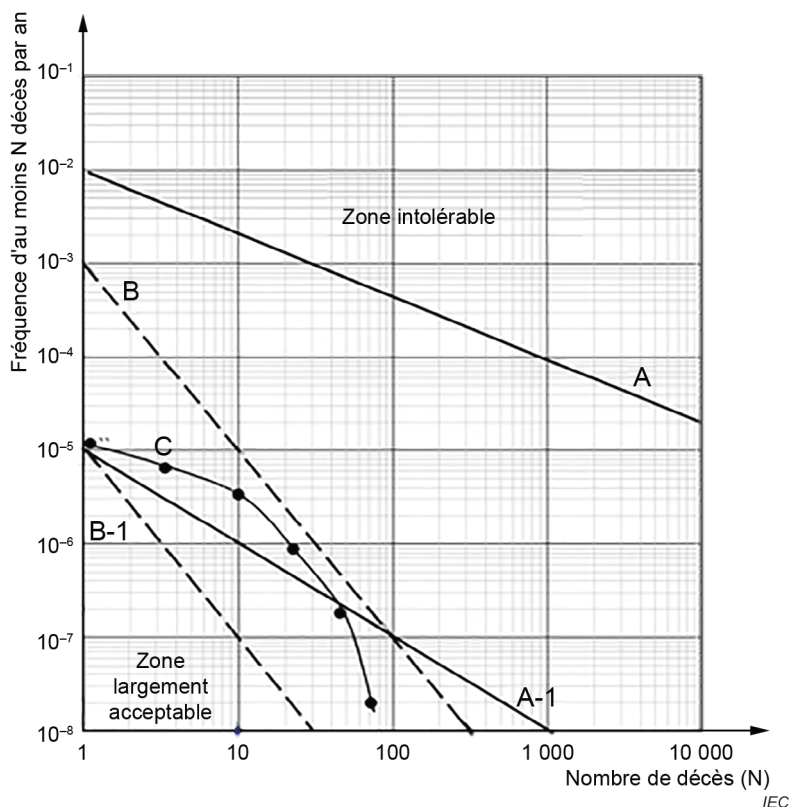


Figure B.13 – Exemple de diagramme F-N

L'application la plus courante est la représentation du risque sociétal provenant des sites de dangers majeurs suggérés, aux fins de l'aménagement du territoire ou d'autres évaluations de sécurité semblables.

NOTE Le risque sociétal fait référence à des préoccupations sociétales dues à la survenance de plusieurs décès au cours d'un même événement.

B.8.3.3 Entrées

Les données d'incidents ou les résultats de l'analyse quantitative du risque, qui permettent de prévoir la probabilité des décès.

B.8.3.4 Résultat

Une représentation graphique des données par rapport aux critères prédéfinis.

B.8.3.5 Avantages et limites

Les avantages des diagrammes F-N incluent ce qui suit.

- Ils offrent un résultat facile à comprendre sur lequel les décisions peuvent s'appuyer;
- L'analyse quantitative nécessaire pour développer un graphique F/N permet de bien comprendre le risque, ses causes et ses conséquences.

Les limites incluent ce qui suit.

- Les calculs permettant de produire les graphiques sont souvent complexes et comprennent de nombreuses incertitudes.
- Une analyse complète exige que tous les scénarios d'accidents majeurs possibles soient analysés. Cela demande beaucoup de temps et exige un degré élevé d'expertise.

- Les diagrammes F-N ne pouvant pas être comparés facilement entre eux afin de réaliser un classement (par exemple, pour décider quel développement représente le risque sociétal le plus élevé).

B.8.3.6 Documents de référence

[72] Understanding and using F-N Diagrams, *Annex in Guidelines for Developing Quantitative Safety Risk Criteria*

[73] EVANS, A. *Transport fatal accidents and FN-curves*

B.8.4 Diagrammes de Pareto

B.8.4.1 Vue d'ensemble

Un diagramme de Pareto (voir Figure B.14) est un outil permettant de choisir un nombre limité de tâches qui produiront un effet global significatif. Il utilise le principe de Pareto (également connu sous le nom de loi des 80/20) qui correspond à l'idée que 80 % des problèmes sont produits par 20 % des causes et qu'en faisant 20 % du travail, 80 % des bénéfices peuvent être générés.

La création d'un diagramme de Pareto pour le choix des causes à traiter comprend les étapes suivantes:

- identifier les problèmes et en dresser une liste;
- identifier la cause de chaque problème;
- regrouper les problèmes selon leur cause commune;
- additionner les scores pour chaque groupe;
- dessiner un diagramme en colonnes qui représente les causes, en faisant apparaître en premier celles qui ont le score le plus élevé.

Le principe de Pareto s'applique au nombre de problèmes et ne tient pas compte de leur importance. C'est-à-dire que des problèmes ayant de graves conséquences peuvent ne pas être associés aux causes les plus courantes de problèmes moins graves. Pour compenser, une pondération peut être apportée en affectant un score aux problèmes en fonction de leurs conséquences. Une analyse de Pareto est une approche ascendante et peut fournir des résultats quantitatifs. Bien que l'application de cette technique ne nécessite aucun outil sophistiqué, ni aucune formation ou compétence particulière, une certaine expérience est très utile pour éviter les limites et les erreurs courantes.

NOTE Les chiffres de 80 % et 20 % sont donnés à titre d'illustration: le principe de Pareto représente le manque de symétrie qui apparaît souvent entre le travail fourni et les résultats obtenus. Par exemple, 13 % du travail pourraient générer 87 % du rendement. Ou 70 % des problèmes pourraient être résolus en traitant 30 % des causes.

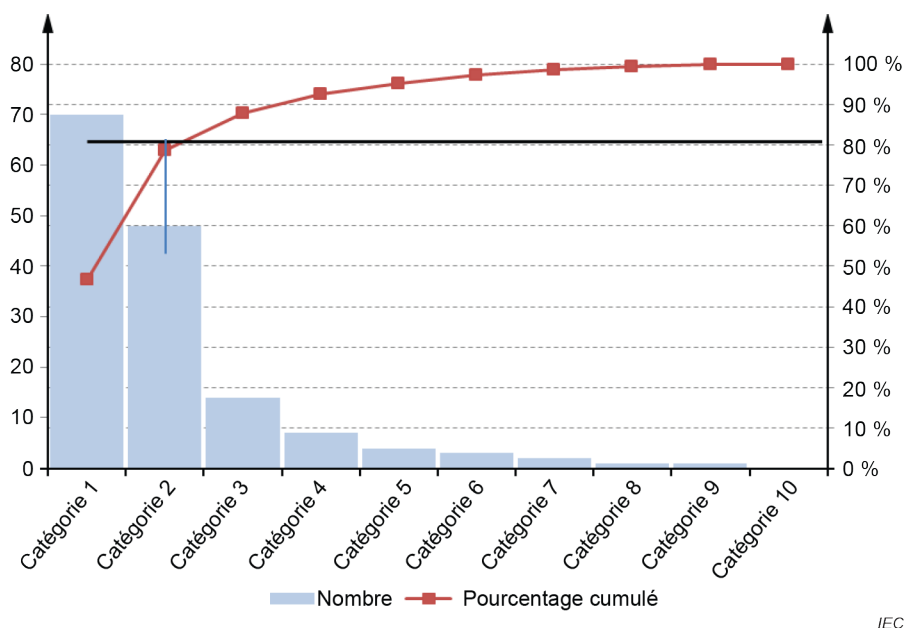


Figure B.14 – Exemple de diagramme de Pareto

B.8.4.2 Utilisation

L'analyse de Pareto est utile au niveau opérationnel, lorsque de nombreux plans d'action sont en concurrence. Elle peut s'appliquer lorsqu'une forme de hiérarchisation est nécessaire. Par exemple, elle peut être utilisée pour aider à décider quelles causes sont les plus importantes à traiter ou quels traitements du risque sont les plus avantageux.

La représentation habituelle d'une analyse de Pareto est un diagramme en barres, où l'axe horizontal représente les catégories considérées (par exemple, les types de matériaux, les dimensions, les codes de rejet, les centres de traitement), plutôt qu'une échelle continue (par exemple, de 0 à 100). Les catégories sont souvent les "défauts", les sources de défauts, ou les entrées dans un processus. L'axe vertical représente un type de comptage ou de fréquence (par exemple, faits, incidents, pièces, temps). Une courbe des pourcentages cumulés est ensuite tracée.

Les catégories à gauche de l'endroit où le cumul des pourcentages croise le repère des 80 % sont celles qui sont traitées.

B.8.4.3 Entrées

Données à analyser, par exemple, les données liées aux réussites et aux échecs passés, ainsi qu'à leurs causes.

B.8.4.4 Résultats

Le résultat est un diagramme de Pareto qui démontre quelles catégories sont les plus significatives, de manière à pouvoir concentrer les efforts sur les zones où les améliorations seront les plus grandes. Un diagramme de Pareto peut aider à déterminer visuellement quelles catégories sont les "quelques éléments essentiels" et lesquelles sont les "nombreux éléments sans importance". Bien que l'analyse soit quantitative, le résultat est une catégorisation des problèmes, des causes, etc. par ordre d'importance.

Si la première analyse contient de nombreux problèmes peu importants ou rares, ils peuvent être regroupés dans la catégorie "autres". Ce groupe apparaît en dernier sur le diagramme de Pareto (même s'il ne s'agit pas de la barre la plus courte). La courbe des contributions en pourcentage cumulé (la somme consécutive des contributions de chaque catégorie sous la forme d'une fraction du total) peut également y figurer.

B.8.4.5 Avantages et limites

Les avantages de l'analyse de Pareto incluent ce qui suit.

- L'analyse de Pareto permet d'examiner les causes communes des risques individuels, ce qui servira de base à l'élaboration d'un plan de traitement.
- Elle fournit un résultat graphique qui indique clairement où les gains peuvent être les plus importants.
- Le temps et les efforts nécessaires pour obtenir des résultats sont probablement modérés à faibles.

Les limites incluent ce qui suit.

- Les coûts ou les difficultés relatives liés au traitement de chaque cause sous-jacente ne sont pas pris en compte.
- Il est nécessaire que les données applicables à la situation analysée soient disponibles.
- Il est nécessaire que les données puissent se diviser en catégories et correspondre à la loi des 80/20 pour que la méthode soit valable.
- Il est difficile de construire des importances relatives lorsque les données sont inadéquates.
- Généralement, seules les données historiques sont prises en compte et aucun changement potentiel n'est envisagé.

B.8.4.6 Documents de référence

[74] *Pareto Chart, Excel Easy*

[75] *Pareto Chart*

B.8.5 Maintenance basée sur la fiabilité (MBF)

B.8.5.1 Vue d'ensemble

La maintenance basée sur la fiabilité (MBF) est une technique d'appréciation basée sur les risques utilisée pour identifier les règles et les tâches de maintenance appropriées pour un système et ses composants, afin d'atteindre de manière efficace et efficiente le niveau de sécurité, de disponibilité et d'économie exigé pour le fonctionnement de tous les types d'équipements. Elle comprend toutes les étapes du processus d'appréciation du risque, y compris l'identification du risque, l'analyse du risque et l'évaluation du risque.

La procédure de base d'un programme MBF est la suivante:

- initiation et planification;
- analyse de défaillance fonctionnelle;
- choix de la tâche de maintenance;
- mise en œuvre;
- amélioration continue.

Dans le cadre de la MBF, l'analyse fonctionnelle est le plus souvent réalisée selon la méthode AMDEC (analyse des modes de défaillance, de leurs effets et de leur criticité, B.2.3) en mettant l'accent sur les situations où les défaillances potentielles peuvent être éliminées ou réduites en fréquence et/ou en conséquences par le biais de tâches de maintenance. Les conséquences sont établies en définissant les effets de la défaillance, puis le risque est analysé en estimant la fréquence de chaque mode de défaillance lorsque la maintenance est omise. Une matrice de risque (B.10.3) permet d'établir des catégories de niveaux de risque.

Les règles de gestion des défaillances appropriées sont alors choisies pour chaque mode de défaillance. Habituellement, le choix des tâches les plus appropriées suit une logique de normalisée.

Un plan est préparé pour mettre en œuvre les tâches de maintenance recommandées. Il définit en détail les tâches, les intervalles entre les tâches, les procédures impliquées, les pièces détachées exigées et les autres ressources nécessaires pour effectuer les tâches de maintenance. Le Tableau B.6 donne un exemple.

L'ensemble du processus MBF est abondamment documenté pour référence et revue ultérieures. La collecte de données liées à la défaillance et à la maintenance permet de surveiller les résultats et la mise en œuvre des améliorations.

B.8.5.2 Utilisation

La MBF est utilisée pour permettre de réaliser une maintenance efficace et effective. Elle est généralement appliquée pendant la phase de conception et de développement d'un système, puis mise en œuvre pendant l'exploitation et la maintenance. Il est plus avantageux de cibler l'analyse sur les cas où les défaillances auraient de graves effets au niveau de la sécurité, de l'environnement, de l'économie ou de l'exploitation.

La MBF est commencée lorsqu'une analyse de criticité de haut niveau a identifié un système et un équipement exigeant des tâches de maintenance à déterminer. Elle peut avoir lieu soit pendant la phase initiale de la conception, soit plus tard, pendant l'utilisation, si elle n'a pas eu lieu de manière structurée avant ou si la maintenance a besoin d'être revue ou améliorée.

B.8.5.3 Entrée

La réussite de l'application de la MBF nécessite une bonne compréhension des équipements et de la structure, de l'environnement d'exploitation et des systèmes, des sous-systèmes et éléments de l'équipement associés, ainsi que des défaillances possibles et leurs conséquences.

Ce processus exige une équipe disposant des connaissances et de l'expérience nécessaires, sous le contrôle d'un animateur formé et expérimenté.

B.8.5.4 Résultat

Le résultat final du processus est un avis relatif à la nécessité de réaliser une tâche de maintenance ou une autre action telle que des modifications fonctionnelles.

Les résultats sont des règles de gestion des défaillances appropriées pour chaque mode de défaillance, par exemple la surveillance des conditions, la recherche de défaillance, la planification de la restauration, le remplacement à intervalle fixe (selon le calendrier, le nombre d'heures d'utilisation ou le nombre de cycles, etc.) ou l'exploitation jusqu'à la défaillance. La reprise de conception, la modification des procédures d'exploitation ou de maintenance ou une formation supplémentaire sont d'autres actions possibles pouvant découler de l'analyse. Le Tableau B.6 donne un exemple.

Un plan est préparé pour la mise en œuvre des tâches de maintenance recommandées. Il décrit les tâches, les intervalles entre les tâches, les procédures concernées, les pièces détachées exigées et les autres ressources nécessaires pour effectuer les tâches de maintenance.

Tableau B.6 – Exemple de choix des tâches avec la MBF

Défaillance fonctionnelle: protection du compresseur et mise à l'arrêt défaillantes							
Equipement	Mode de défaillance	Intervalle de défaillance (heures)	Détection de la défaillance	Causes	Type de tâche	Description de la tâche	Intervalle entre les tâches en heures
Transmetteur de pression – pression d'huile dans le compresseur	Sortie inexacte	80 000	Evidente	Hors tolérance	Conditionnée par le temps	Vérifier l'étalonnage	16 000
Capteur de vibrations – vibration du compresseur	Ne fournit pas la sortie correcte	40 000	Evidente	Défaillance du détecteur/ capteur	Conditionnée par l'état	Vérifier l'exactitude en cas de variation des vibrations	En permanence sur le panneau de commande
Contacteur de niveau – faible niveau d'huile dans le compresseur	Ne change pas d'état à la demande	80 000	Cachée	Défaillance du détecteur/ capteur	Recherche de défaillance	Essai fonctionnel sur le contacteur de niveau	8 000
Capteur et câblage – température de l'huile du compresseur	Sortie élevée	160 000	Evidente	Circuit ouvert	Conditionnée par le temps	Rechercher les raccords desserrés	8 000
Transmetteur de niveau – réservoir de glycol	Sortie inexacte	40 000	Cachée	Hors tolérance	Conditionnée par le temps	Etalonner le transmetteur après avoir vérifié le niveau de remplissage de glycol	8 000
Transmetteur de pression – pression d'aspiration/de refoulement du compresseur	Sortie inexacte	80 000	Evidente	Hors tolérance	Conditionnée par le temps	Vérifier l'étalonnage	16 000
Capteur et câblage – température d'aspiration/de refoulement du compresseur	Sortie élevée	160 000	Evidente	Circuit ouvert	Conditionnée par le temps	Rechercher les raccords desserrés	8 000
Capteur de vibrations – vibration du refroidisseur	Ne fournit pas la sortie correcte	40 000	Evidente	Défaillance du détecteur/ capteur	Conditionnée par l'état	Vérifier l'exactitude en cas de variation des vibrations	En permanence sur le panneau de commande

B.8.5.5 Avantages et limites

Les avantages incluent ce qui suit.

- Ce processus permet d'utiliser l'ampleur du risque pour prendre des décisions concernant la maintenance.
- Les tâches sont choisies suivant leur applicabilité, c'est-à-dire si elles permettront d'obtenir le résultat escompté.
- Les tâches sont évaluées pour s'assurer que leur application sera rentable et utile.
- Les actions de maintenance inutiles sont éliminées et leur élimination est correctement justifiée.
- Le processus et les décisions sont documentés pour revue ultérieure.

Les limites incluent ce qui suit.

- Pour être efficace, le processus prend généralement du temps.
- Le processus repose grandement sur la présence d'un animateur formé et expérimenté.
- L'équipe doit avoir toute l'expertise nécessaire et l'expérience de la maintenance pour que ses décisions soient valables.
- Il peut y avoir une tendance à prendre des raccourcis pendant le processus, ce qui affecte la validité des décisions prises.
- Les tâches potentielles à l'étude seront limitées par les connaissances relatives aux techniques disponibles, par exemple celles qui concernent la surveillance des conditions.

B.8.5.6 Document de référence

[76] IEC 60300-3-11, *Gestion de la sûreté de fonctionnement – Partie 3-11: Guide d'application – Maintenance basée sur la fiabilité*

B.8.6 Indices de risque

B.8.6.1 Vue d'ensemble

Les indices de risque fournissent une mesure des risques déduite à l'aide d'une approche de pointage et d'échelles ordinales. Les facteurs réputés comme ayant de l'influence sur l'ampleur du risque sont identifiés, notés et combinés à l'aide d'une équation qui vise à représenter leurs relations. Dans les formules les plus simples, les facteurs qui augmentent le niveau de risque sont multipliés entre eux et divisés par ceux qui réduisent le niveau de risque. Dans la mesure du possible, les échelles et la manière dont elles sont combinées s'appuient sur des preuves et sur des données.

Il est important d'assurer la cohérence et la relativité internes des pointages de chaque partie du système.

Les formules mathématiques ne peuvent pas être appliquées aux échelles ordinales. Par conséquent, après le développement du système de pointage, il convient de valider le modèle en l'appliquant à un système qui est bien compris.

Le développement d'un indice est une approche itérative, et il convient d'essayer plusieurs systèmes différents de combinaisons des pointages pour valider la méthode.

B.8.6.2 Utilisation

En substance, les indices de risque représentent une approche qualitative ou semi-quantitative du classement et de la comparaison des risques. Ils peuvent être utilisés pour les risques internes et externes d'un domaine d'application limité ou étendu. Ils sont souvent spécifiques à un type de risque particulier et utilisés pour comparer différentes situations où ce risque survient. Les nombres sont utilisés simplement pour tenir compte de la

manipulation. Dans les cas où le modèle ou le système sous-jacent n'est pas bien connu ou ne peut pas être représenté, il est habituellement plus avantageux d'utiliser une approche plus ouvertement qualitative qui n'implique pas un niveau d'exactitude qui est impossible avec les échelles ordinales.

EXEMPLE 1 Un indice de risque de maladie est utilisé pour estimer le risque pour un individu de contracter une maladie particulière en combinant les notes de plusieurs facteurs de risque connus identifiés dans les études épidémiologiques, en tenant compte de la force de l'association entre le facteur de risque et la maladie.

EXEMPLE 2 Les cotes de danger de feux de brousse comparent le risque d'incendie sur plusieurs jours en tenant compte des conditions prévues comme l'humidité, la force du vent, la sécheresse du paysage et la charge de combustible.

EXEMPLE 3 Les prêteurs calculent les risques de crédits pour leurs clients en utilisant des indices qui représentent les composants de leur stabilité financière.

B.8.6.3 Entrées

Les entrées sont déduites de l'analyse du système. Cela exige une bonne compréhension de toutes les sources du risque et de la manière dont les conséquences peuvent survenir.

Les outils comme l'AAP (B.5.7), l'AAE (B.5.6) et l'ACM (B.9.5) peuvent être utilisés, ainsi que les données historiques pour venir à l'appui du développement des indices de risques.

Etant donné que le choix de l'échelle ordinale utilisée est, dans une certaine mesure, arbitraire, des données suffisantes sont nécessaires à la validation de l'indice.

B.8.6.4 Résultat

Le résultat est une série de nombres (indices composites) liée à un risque particulier et pouvant être comparée aux indices développés pour d'autres risques à l'intérieur du même système.

B.8.6.5 Avantages et limites

Les avantages des indices de risques incluent ce qui suit.

- Ils peuvent être un outil de pointage simple et facile à utiliser pour le classement des différents risques.
- Ils permettent d'intégrer plusieurs facteurs ayant un impact sur le niveau de risque dans un seul pointage numérique.

Les limites incluent ce qui suit.

- Si le processus (modèle) et son résultat ne sont pas correctement validés, les résultats peuvent être dépourvus de sens.
- Le fait que le résultat soit une valeur numérique du risque peut prêter à interprétation et utilisation erronées, dans l'analyse coût/bénéfice subséquente, par exemple.
- Dans la plupart des cas, lorsque les indices sont utilisés, aucun modèle fondamental ne permet de déterminer si les échelles individuelles des facteurs de risque sont linéaires, logarithmiques ou autre, ni de déterminer la manière dont il convient de combiner ces facteurs. Dans ces situations, le classement est naturellement peu fiable et la validation par rapport à des données réelles est particulièrement importante.
- Il est souvent difficile d'obtenir des preuves suffisantes pour valider les échelles.
- L'utilisation de valeurs numériques peut entraîner un niveau d'exactitude qui ne peut pas être justifié.

B.8.6.6 Document de référence

[77] MACKENZIE Cameron A. *Summarizing risk using risk measures and risk indices*

B.9 Techniques de choix parmi des options

B.9.1 Généralités

Les techniques de l'Article B.9 sont utilisées pour aider les décideurs à choisir parmi des options qui impliquent de multiples risques et où il est nécessaire de faire des compromis. Ces techniques aident à fournir une base logique pour justifier les raisons d'une décision. Puisque chaque méthode correspond à une philosophie différente, il peut être utile d'explorer les options en utilisant plus d'une méthode.

Avec l'analyse par arbre de décision et l'analyse coût/bénéfice, les décisions s'appuient sur les pertes ou les gains financiers attendus. L'analyse à critères multiples permet de pondérer différents critères et de faire des compromis. L'analyse de scénario (voir B.2.5) peut également être utilisée pour explorer les conséquences possibles si différentes options sont suivies. Cette méthode est particulièrement utile en présence d'un niveau élevé d'incertitude. Les problèmes décisionnels peuvent également être modélisés à l'aide de diagrammes d'influence (B.5.3).

B.9.2 Analyse coût/bénéfice (ACB)

B.9.2.1 Vue d'ensemble

L'analyse coût/bénéfice met en balance les coûts totaux attendus des options en des termes monétaires et leurs bénéfices totaux attendus, afin de choisir l'option la plus rentable ou la plus avantageuse. Elle peut être qualitative ou quantitative, ou bien combiner des éléments quantitatifs et qualitatifs, et elle peut s'appliquer à tous les niveaux d'une organisation.

Les parties prenantes qui pourraient subir des coûts ou recevoir des bénéfices (tangibles ou intangibles) sont identifiées avec les bénéfices et les coûts directs et indirects qui les concernent.

NOTE Les coûts directs sont les coûts directement associés à l'action. Les coûts indirects sont les coûts supplémentaires d'opportunité, tels que la perte d'utilité, le risque de gaspiller du temps de gestion ou le détournement du capital loin d'autres investissements potentiels.

Dans l'ACB quantitative, une valeur monétaire est assignée à tous les coûts et bénéfices tangibles et intangibles. Il arrive souvent que le coût soit engagé sur une courte période (par exemple, un an) et que les bénéfices affluent pendant une longue période. Il est alors nécessaire d'actualiser les coûts et les bénéfices pour les ramener en "monnaie courante" de manière à pouvoir obtenir une comparaison valide entre les coûts et les bénéfices. La valeur actualisée de tous les coûts (VAC) et la valeur actualisée de tous les bénéfices (VAB) vis-à-vis de toutes les parties prenantes peuvent être combinées pour générer une valeur actualisée nette (VAN): $VAN = VAB - VAC$.

Une VAN positive indique que l'action pourrait être une option convenable. L'option qui présente la VAN la plus élevée n'est pas nécessairement l'option la plus avantageuse. Le rapport le plus élevé entre la VAN et la valeur actualisée des coûts est un indicateur utile pour connaître l'option la plus avantageuse. Il convient de combiner un choix basé sur l'ACB avec un choix stratégique entre des options satisfaisantes qui pourraient offrir individuellement des coûts de traitement inférieurs, des bénéfices plus importants ou un résultat plus avantageux (meilleur rendement du capital investi). Un tel choix stratégique peut être exigé au niveau des politiques et au niveau opérationnel.

L'incertitude liée aux coûts et aux bénéfices peut être prise en compte en calculant la moyenne pondérée par la probabilité des bénéfices nets (la valeur actualisée nette attendue ou VANA). Dans ce calcul, il est admis par hypothèse que l'utilisateur n'a pas de préférence entre une faible récompense avec une forte probabilité de récurrence et une récompense élevée avec une faible probabilité de récurrence, dès lors que les deux options ont la même valeur attendue. Les calculs de la VAN peuvent également être combinés avec des arbres de décision (B.9.3) pour modéliser l'incertitude dans les décisions à venir et leurs résultats. Dans certains cas, il est possible de reporter certains coûts jusqu'à ce que de meilleures

informations soient disponibles concernant les coûts et les bénéfices. Cette possibilité a une valeur qui peut être estimée à l'aide de l'analyse par les options réelles.

L'ACB qualitative ne tente pas d'attribuer une valeur pécuniaire aux coûts irrécupérables, et plutôt que de fournir une seule valeur cumulant les coûts et les bénéfices, elle examine d'un point de vue qualitatif les relations et les compromis qui existent entre les différents coûts et bénéfices.

Une technique connexe est une analyse coût-efficacité. Elle prend pour hypothèse qu'un avantage ou un résultat donné est souhaité, et qu'il existe plusieurs moyens alternatifs pour l'obtenir. L'analyse ne s'intéresse qu'aux coûts et cherche à identifier la manière la moins onéreuse d'obtenir l'avantage envisagé.

Bien que les valeurs intangibles soient souvent traitées en leur attribuant une valeur pécuniaire, un facteur de pondération peut également être appliqué aux autres coûts, par exemple pour donner plus de poids aux avantages de sécurité qu'aux avantages financiers.

Une variante de l'ACB – analyse coût/bénéfice/risque (ACBR) – met davantage l'accent sur les risques. Contrairement à l'ACB qui utilise des distributions ponctuelles ou binaires, dans le modèle ACBR la valeur du risque peut également prendre en compte des distributions de probabilités complètes couvrant les conséquences négatives et positives [78].

B.9.2.2 Utilisation

L'ACB est utilisée au niveau opérationnel et au niveau stratégique pour aider à choisir entre plusieurs options. Dans la plupart des cas, ces options contiendront une incertitude. La variabilité de la valeur actualisée attendue des coûts et des bénéfices, ainsi que la possibilité d'événements imprévus nécessitent d'être prises en compte dans les calculs. Une analyse de sensibilité ou une analyse de Monte-Carlo (B.5.10) peut être utilisée à cet effet.

L'ACB peut aussi être utilisée pour la prise de décision concernant les risques et leur traitement, par exemple:

- comme entrée pour décider s'il convient de traiter ou non un risque;
- pour choisir les meilleures formes de traitement du risque;
- pour comparer les options de traitement à long terme et à court terme.

B.9.2.3 Entrées

Les entrées comprennent des informations sur les coûts et bénéfices vis-à-vis des parties prenantes correspondantes et sur les incertitudes liées à ces coûts et bénéfices. Il convient de tenir compte des coûts récupérables et irrécupérables et des bénéfices. Les coûts comprennent toutes les ressources qui pourraient être consommées, y compris les coûts directs et indirects, les frais généraux attribuables et les impacts négatifs. Les bénéfices comprennent les impacts positifs et l'évitement des coûts (qui peut résulter du traitement du risque). Les coûts irrécupérables déjà engagés ne font pas partie de cette analyse. Une simple analyse par feuille de calcul ou une discussion qualitative ne demande pas d'effort substantiel, mais l'application aux problèmes les plus complexes implique de passer beaucoup de temps à collecter les données nécessaires et à estimer une valeur pécuniaire convenable pour les valeurs intangibles.

B.9.2.4 Résultat

Le résultat d'une analyse coût-bénéfice est une information sur les coûts et bénéfices relatifs en fonction de différentes options ou actions. Il peut être exprimé de manière quantitative par une valeur actualisée nette (VAN), par le meilleur rapport (VAN/VAC) ou par le rapport de la valeur actualisée des bénéfices à la valeur actualisée des coûts.

Le résultat qualitatif se traduit généralement par un tableau de comparaison des coûts et des bénéfices de différents types tenant particulièrement compte des compromis.

B.9.2.5 Avantages et limites

Les avantages de l'analyse ACB incluent ce qui suit.

- L'ACB permet de comparer les coûts et les bénéfices selon une métrique simple (généralement numéraire).
- Elle offre la transparence des informations utilisées pour orienter les décisions.
- Elle encourage la collecte d'informations détaillées concernant tous les aspects possibles de la décision (ce qui peut être utile pour révéler les lacunes et pour transmettre les connaissances).

Les limites incluent ce qui suit.

- L'ACB exige une bonne compréhension des bénéfices probables, ce qui la rend mal adaptée aux situations nouvelles ayant un niveau élevé d'incertitude;
- L'analyse coût/bénéfice quantitative peut produire des chiffres significativement différents en fonction des hypothèses et des méthodes utilisées pour attribuer des valeurs économiques à des avantages non économiques et intangibles.
- Pour certaines applications, il est difficile de définir un taux d'actualisation valide pour les coûts et bénéfices futurs.
- Les bénéfices dont profite une large population sont difficiles à estimer, notamment ceux liés au bien-être public qui ne fait pas l'objet d'échange sur les marchés. Toutefois, combinés à la "volonté de payer ou d'accepter", ces bénéfices externes ou sociétaux peuvent être pris en compte.
- Selon le taux d'actualisation choisi, la pratique de l'actualisation signifie que les bénéfices obtenus sur le long terme peuvent avoir une influence négligeable sur les décisions, ce qui décourage l'investissement à long terme.
- L'ACB traite mal l'incertitude concernant la temporalité de la survenue des coûts et des bénéfices ou la souplesse dans les prises de décision futures.

B.9.2.6 Documents de référence

[79] *The Green book, Appraisal and Evaluation in Central Government*

[80] ANDOSEH, S., et al. *The case for a real options approach to ex-ante cost-benefit analyses of agricultural research projects*

B.9.3 Analyse par arbre de décision

B.9.3.1 Vue d'ensemble

Un arbre de décision modélise les cheminements possibles qui suivent une décision initiale qui doit être prise (par exemple, suivre le Projet A ou le Projet B). À mesure du déroulement des deux projets hypothétiques, différents événements pourraient se produire et il sera nécessaire de prendre différentes décisions prévisibles. Ce processus est représenté dans une arborescence s'apparentant à un arbre d'événement. La probabilité des événements peut être estimée, ainsi que la valeur attendue ou l'utilité du résultat final de chaque cheminement.

Logiquement, les informations relatives au meilleur cheminement de décision sont celles qui produisent la meilleure valeur probable, calculée comme le produit de toutes les probabilités conditionnelles tout au long du cheminement et de la valeur du résultat.

B.9.3.2 Utilisation

L'arbre de décision peut être utilisé pour structurer et résoudre des problèmes décisionnels séquentiels, et il est particulièrement avantageux lorsque la complexité du problème croît. Il permet à une organisation de quantifier les résultats possibles des décisions, et aide donc les décideurs à choisir les meilleures actions lorsque les résultats sont incertains. L'affichage graphique peut également permettre de mieux transmettre les raisons justifiant des décisions.

Il est utilisé pour évaluer une décision suggérée, souvent à l'aide d'une estimation subjective des probabilités des événements, et aide les décideurs à dépasser les partis pris qui leur sont propres, concernant l'échec ou la réussite. Il peut être utilisé pour les problèmes à court, moyen et long terme, au niveau opérationnel ou stratégique.

B.9.3.3 Entrées

Le développement d'un arbre de décision exige un plan du projet avec des points de décision, des informations concernant les résultats possibles de ces décisions et concernant les éventuels événements qui pourraient affecter les décisions. Une expertise est nécessaire pour mettre l'arbre en place correctement, en particulier dans les situations complexes.

Selon la construction de l'arbre, des données quantitatives ou des informations suffisantes sont nécessaires pour justifier l'avis d'expert concernant les probabilités.

B.9.3.4 Résultats

Les résultats comprennent:

- une représentation graphique du problème décisionnel;
- un calcul de la valeur prévue pour chaque cheminement possible;
- une liste hiérarchisée des résultats possibles en fonction de la valeur attendue ou du cheminement recommandé à suivre.

B.9.3.5 Avantages et limites

Les avantages de l'analyse par arbre de décision incluent ce qui suit.

- Elle offre une représentation graphique claire des détails d'un problème décisionnel.
- L'exercice du développement de l'arbre de décision peut conduire à une meilleure connaissance du problème.
- Elle favorise la clarté de la réflexion et de la planification.
- Elle permet de calculer le meilleur cheminement pour résoudre une situation, ainsi que le résultat attendu.

Les limites incluent ce qui suit.

- Les arbres de décision de grande taille peuvent se révéler trop complexes et rendre de ce fait la communication difficile.
- On peut avoir tendance à simplifier exagérément la situation pour pouvoir la représenter dans une arborescence.
- Elle s'appuie sur des données historiques qui pourraient ne pas s'appliquer à la décision modélisée.
- Elle simplifie les résultats des problèmes décisionnels qui la discrétisent, ce qui élimine les valeurs extrêmes.

B.9.3.6 Document de référence

[81] KIRKWOOD Craig, *Decision Tree Primer*

B.9.4 Théorie des jeux

B.9.4.1 Vue d'ensemble

B.9.4.1.1 Généralités

La théorie des jeux est un moyen de modéliser les conséquences de différentes décisions possibles selon un certain nombre de situations futures possibles. Les situations futures peuvent être déterminées par un décideur différent (par exemple, un concurrent) ou par un événement externe comme l'échec ou la réussite d'une technologie ou d'un essai. Par hypothèse, la tâche consiste à déterminer le prix d'un produit en tenant compte des différentes décisions qui pourraient être prises par les différents décideurs (appelés joueurs) à différents moments. La rentabilité pour chaque joueur participant au jeu, par rapport à la période concernée, peut être calculée et la stratégie qui présente la récompense optimale pour chaque joueur peut être choisie. La théorie des jeux peut également être utilisée pour déterminer la valeur des informations concernant l'autre joueur ou les différents résultats possibles (par exemple, la réussite d'une technologie).

Il existe différents types de jeux, par exemple coopératifs/non coopératifs, symétriques/asymétriques, à somme nulle/à somme non nulle, simultanés/séquentiels, à information parfaite/à information imparfaite, les jeux combinatoires, les résultats stochastiques.

B.9.4.1.2 Communication et jeux coopératifs/non coopératifs

Le fait que la communication entre les joueurs soit possible, admise ou non est un facteur important. Un jeu est coopératif si les joueurs peuvent prendre des engagements à caractère obligatoire. Dans les jeux non coopératifs, cela n'est pas possible. Les jeux hybrides contiennent des éléments coopératifs et non coopératifs. Par exemple, les joueurs forment des coalitions dans un jeu coopératif, mais ils jouent de manière non coopérative.

L'exemple classique des jeux sans communication entre les joueurs est le "dilemme du prisonnier". Il montre que dans certains cas, le fait que chaque joueur agisse en vue d'améliorer son propre résultat sans se soucier de l'autre peut entraîner la situation la plus défavorable pour les deux. Ce type de jeu a été utilisé pour analyser les conflits et la coopération entre deux joueurs lorsque le manque de communication peut conduire à une situation instable, qui pourrait entraîner le résultat le plus défavorable possible pour les deux joueurs. Dans le jeu du dilemme du prisonnier, par hypothèse, deux personnes ont commis un crime ensemble. Elles sont séparées et ne peuvent pas communiquer. La police propose un marché. Si chaque prisonnier admet sa culpabilité et témoigne contre l'autre, il recevra une sentence amoindrie, mais l'autre prisonnier verra sa peine augmentée. Un prisonnier reçoit la peine maximale s'il refuse d'avouer et de témoigner, mais que l'autre accepte. Ainsi, pour améliorer leur situation, les deux sont tentés d'avouer et de témoigner, mais dans ce cas, les deux recevront la peine maximale. Leur meilleure stratégie consisterait à refuser le marché et ne rien avouer. Dans ce cas, ils recevraient tous les deux la peine minimale.

B.9.4.1.3 Jeux à somme nulle/à somme non nulle et symétriques/asymétriques

Dans un jeu à somme nulle, un joueur gagne ce que l'autre perd. Dans un jeu à somme non nulle, la somme des résultats peut varier en fonction des décisions. Par exemple, le fait de réduire les prix peut coûter davantage à un joueur qu'à l'autre, mais cela peut augmenter le volume du marché pour les deux.

B.9.4.1.4 Jeux simultanés/séquentiels

Dans certains jeux, le calcul concerne seulement une interaction entre les joueurs. Mais, dans les jeux séquentiels, les joueurs interagissent plusieurs fois et peuvent changer de stratégie d'une partie à l'autre.

Par exemple, des simulations ont été réalisées pour étudier les effets de la triche sur un marché. Chaque joueur a deux possibilités. Le fournisseur peut livrer ou ne pas livrer et le client peut payer ou ne pas payer. Parmi les quatre résultats possibles, le résultat normal avantage les deux joueurs (le fournisseur livre et le client paye). Le résultat où le fournisseur ne livre pas et où le client ne paye pas est une occasion manquée. Les deux dernières possibilités entraînent une perte pour le fournisseur (le client ne paye pas) ou pour le client (le fournisseur ne livre pas). La simulation a permis de soumettre à essai différentes stratégies comme le fait de toujours jouer honnêtement, le fait de toujours tricher ou le fait de tricher de manière aléatoire. La simulation a permis de déterminer que la stratégie optimale consistait à jouer honnêtement lors de la première interaction et à copier le comportement de l'autre joueur au tour suivant (jouer honnêtement ou tricher).

NOTE Dans la réalité, le fournisseur démasquerait probablement le client tricheur, et il arrêterait de jouer avec lui.

B.9.4.2 Utilisation

La théorie des jeux permet d'évaluer le risque dans les cas où le résultat d'un certain nombre de décisions dépend de l'action d'un autre joueur (par exemple, un concurrent) ou d'un certain nombre de résultats possibles (par exemple, si une nouvelle technologie fonctionnera ou pas). Les exemples suivants montrent les informations qui peuvent être obtenues grâce à l'analyse par la théorie des jeux.

Le Tableau B.7 montre une situation où une entreprise peut choisir entre trois technologies différentes. Mais les bénéfices dépendront de l'action d'un concurrent (action 1, 2 ou 3). L'action que le concurrent choisira est inconnue, mais les probabilités sont estimées selon les indications. Les bénéfices, en millions d'unités monétaires (UM), sont calculés dans le tableau.

Tableau B.7 – Exemple de matrice de jeu

	Concurrent			Bénéfices attendus	Bénéfices garantis	Regret maximal
	Action 1	Action 2	Action 3			
Probabilité	0,4	0,5	0,1			
Technologie 1	0,10	0,50	0,90	0,38	0,10	0,50
Technologie 2	0,50	0,50	0,50	0,50	0,50	0,40
Technologie 3	0,60	0,60	0,30	0,57	0,30	0,60

Les informations suivantes peuvent être extraites du tableau pour appuyer la décision.

Clairement, la technologie 3 est la meilleure, avec des bénéfices attendus de 0,57 million d'UM. Mais il convient de tenir compte de sa sensibilité à l'action du concurrent. La colonne des bénéfices garantis indique que pour une technologie donnée, les bénéfices seront indépendants de ce que fait le concurrent. Ici, la technologie 2 est la meilleure, avec des bénéfices garantis de 0,50 million d'UM. Il convient de se demander s'il est pertinent de choisir la technologie 3 pour gagner seulement 0,07 million d'UM en risquant de perdre 0,20 million d'UM.

Le regret maximal peut en outre être calculé, c'est-à-dire la différence entre les bénéfices obtenus en choisissant une technologie donnée et les bénéfices possibles en connaissant l'action du concurrent. Ce calcul donne les bénéfices pécuniaires dérivés d'une meilleure connaissance de la décision du concurrent. Cette meilleure connaissance peut être obtenue par le biais d'une négociation ou par d'autres moyens légaux. Dans cet exemple, la valeur du supplément d'informations est la plus grande pour la technologie 3.

B.9.4.3 Entrées

Pour que le jeu soit entièrement défini, les éléments suivants doivent être spécifiés comme entrées, au minimum:

- les joueurs ou les alternatives qui constituent le jeu;
- les informations et les actions disponibles pour chaque joueur à chaque point de décision.

B.9.4.4 Résultat

Le résultat est la récompense pour chaque option du jeu, généralement prise pour représenter l'utilité de chaque joueur. Souvent, dans les situations de modélisation, les récompenses représentent de l'argent, mais d'autres résultats sont possibles (par exemple, une part de marché ou le retard d'un projet)

B.9.4.5 Avantages et limites

Les avantages de la théorie des jeux incluent ce qui suit.

- Elle développe un cadre organisationnel permettant d'analyser la prise de décision lorsque plusieurs décisions sont possibles, mais que le résultat dépend de la décision d'un autre joueur ou du résultat d'un événement futur.
- Elle développe un cadre organisationnel permettant d'analyser la prise de décision dans les situations où l'interdépendance des décisions prises par différentes organisations est prise en compte.
- Elle donne un aperçu de plusieurs concepts moins connus survenant en cas de conflit d'intérêts; par exemple, elle décrit et explique les phénomènes du marchandage et de la formation de coalitions.
- Dans les jeux à somme nulle entre deux organisations au moins, la théorie des jeux expose les grandes lignes d'une technique quantitative scientifique qui peut être utilisée par les joueurs pour parvenir à une stratégie optimale.

Les limites incluent ce qui suit.

- Il est pris pour hypothèse que les joueurs ont connaissance de leurs propres récompenses et que les actions et récompenses des autres pourrait manquer de réalisme.
- Les techniques de résolution des jeux où les stratégies sont mixtes (en particulier pour une matrice contenant des récompenses élevées) sont très compliquées.
- Tous les problèmes liés à la concurrence ne peuvent pas être analysés à l'aide de la théorie des jeux.

B.9.4.6 Documents de référence

[82] MYERSON, ROGER B., *Game Theory: Analysis of Conflict*

[83] MARYNARD, SMITH JOHN, *Evolution and Theory of Games*

[84] ROSENHEAD, J. and MINGER, J. (Eds), *Rational Analysis for a Problematic World Revisited*

B.9.5 Analyse à critères multiples (ACM)

B.9.5.1 Vue d'ensemble

L'ACM utilise différents critères pour apprécier et comparer de manière transparente les performances globales d'un ensemble d'options. D'une manière générale, l'objectif est de produire un ordre de préférence pour un ensemble d'options. L'analyse implique l'élaboration d'une matrice d'options et de critères qui sont classés et agrégés pour fournir un pointage global pour chaque option. Ces techniques sont également connues sous le nom de prise de décision multiattribut (ou à attributs multiples) ou multiobjectif. Il existe de nombreuses variantes de cette technique, et de nombreuses applications logicielles à l'appui.

En règle générale, une personne ou un groupe de parties prenantes bien informées réalise le processus suivant:

- définition de l'objectif/des objectifs; détermination des attributs (critères ou mesures de performance fonctionnelle) liés à chaque objectif;
- structuration des attributs selon une hiérarchie des exigences nécessaires et souhaitées;
- détermination de l'importance de chaque critère et attribution des facteurs de pondération de chacun;
- obtention du consensus des parties prenantes concernant la hiérarchie pondérée;
- évaluation des alternatives concernant les critères (cela peut se représenter sous forme d'une matrice de pointages);
- combinaison de plusieurs pointages à attribut simple en un pointage global pondéré à attributs multiples;
- évaluation des résultats pour chaque option;
- appréciation de la fiabilité du classement des options en effectuant une revue de la sensibilité afin d'explorer l'impact d'une modification des pondérations de la hiérarchie des attributs.

Différentes méthodes permettent d'obtenir la pondération pouvant être appliquée à chaque critère et les différentes manières d'agréger les pointages relatifs aux critères pour chaque option en un seul pointage à attributs multiples. Par exemple, les pointages peuvent être agrégés par une somme pondérée ou un produit pondéré, ou en utilisant une méthode de hiérarchie multicritère (il s'agit d'une technique de stimulation en faveur des facteurs de pondération et des pointages, fondée sur des comparaisons par paires). Toutes ces méthodes prennent pour hypothèse que la préférence accordée à un critère ne dépend pas des valeurs des autres critères. Lorsque cette hypothèse n'est pas valide, différents modèles sont utilisés.

Dans la mesure où les pointages sont subjectifs, l'analyse de sensibilité permet d'examiner la mesure dans laquelle les facteurs de pondération et les pointages ont un effet sur les préférences globales accordées aux différentes options.

B.9.5.2 Utilisation

L'ACM peut être utilisée pour:

- comparer plusieurs options dans le cadre d'une première analyse pour déterminer les options préférentielles et inadéquates;
- comparer les options lorsque les critères sont multiples, et parfois en contradiction;
- parvenir à un consensus sur une décision lorsque les objectifs ou les valeurs des différentes parties prenantes sont en contradiction.

B.9.5.3 Entrées

Les entrées sont un ensemble d'options d'analyse et de critères, selon les objectifs, pouvant être utilisés pour apprécier les performances des options.

B.9.5.4 Résultats

Les résultats peuvent être les présentés dans:

- un classement ordonné des options préférentielles, des meilleures aux moins bonnes;
- une matrice où les axes représentent la pondération des critères et le pointage des critères pour chaque option.

La présentation des résultats dans une matrice permet d'éliminer les options qui ne répondent pas aux critères ayant le plus de poids ou à un critère nécessaire.

B.9.5.5 Avantages et limites

Les avantages de l'ACM incluent ce qui suit.

- Elle peut fournir une structure simple pour une prise de décision efficace et une présentation des hypothèses et des conclusions.
- Elle peut rendre plus gérables les problèmes décisionnels complexes qui ne peuvent pas faire l'objet d'une analyse coût/bénéfice.
- Elle peut envisager les problèmes de manière rationnelle lorsqu'il est nécessaire de faire des compromis.
- Elle peut aider à parvenir à un accord lorsque les parties prenantes ont des objectifs divergents, et de ce fait, des valeurs et des critères différents.

Les limites incluent ce qui suit.

- L'ACM peut être affectée par les partis pris et par un mauvais choix des critères de décision.
- Les algorithmes d'agrégation qui calculent les facteurs de pondération des critères à partir des préférences déclarées ou qui agrègent différents points de vue peuvent masquer le véritable fondement de la décision;
- Le système de pointage peut simplifier exagérément le problème décisionnel.

B.9.5.6 Documents de référence

- [85] EN 16271:2012, *Management par la valeur – Expression fonctionnelle du besoin et cahier des charges fonctionnel – Exigences pour l'expression et la validation du besoin à satisfaire dans le processus d'acquisition ou d'obtention d'un produit*

NOTE L'EN 16271:2012 présente les approches permettant de réconcilier les besoins contradictoires des parties prenantes, les méthodes qui peuvent être utilisées pour déduire les exigences en matière de performances fonctionnelles et des recommandations permettant de fixer la granularité de l'analyse à critères multiples avant de comparer les options.

- [86] DEPARTMENT FOR COMMUNITIES AND LOCAL GOVERNMENT, *Multi-criteria analysis: a manual* 2009
- [87] RABIHAH MHD.SUM (2001), *Risk Management Decision Making*
- [88] VELASQUEZ, M., HESTER, P. *An Analysis of Multi-criteria Decision Making Methods*

B.10 Techniques d'enregistrement et de consignation

B.10.1 Généralités

L'Article B.10 couvre les techniques utilisées pour rapporter et consigner les informations générales concernant les risques. Les exigences relatives aux rapports détaillés sont traitées en 6.6.

Une approche commune de la manière de rapporter et de consigner les informations concernant les risques consiste à entrer les informations de base concernant chaque risque dans un registre des risques, par exemple une feuille de calcul ou une base de données (voir B.10.2). Certains risques peuvent exiger une description plus complexe que ce qui entre dans un registre de risques classique. Par exemple, il se peut qu'il soit nécessaire qu'une description inclue plusieurs sources de risques menant à un seul événement, plusieurs résultats découlant d'un même événement ou d'une même source, de répercussions et de possibles défaillances des moyens de maîtrise. Le diagramme "nœud papillon" est un exemple d'outil pouvant être utilisé pour organiser et pour transmettre ce type d'informations (voir B.4.2).

Les informations concernant l'amplitude du risque peuvent aussi être rapportées de différentes manières. La méthode la plus courante utilise une matrice conséquence/vraisemblance (voir B.10.3). Comme la vraisemblance, la conséquence et le

niveau de risque indiqués par leur position dans la matrice, des informations supplémentaires comme la nature des moyens de maîtrise, la mesure dans laquelle les traitements ont été mis en œuvre, etc. peuvent être fournies par la taille des points qui marquent le risque ou leur couleur.

Dans la matrice conséquence/vraisemblance, il est exigé qu'un risque puisse être représenté par une seule paire conséquence/vraisemblance. Les risques, lorsque ce n'est pas le cas, peuvent parfois être représentés par une fonction de distribution de la probabilité ou par une fonction de distribution cumulative (voir B.10.4).

B.10.2 Registres des risques

B.10.2.1 Vue d'ensemble

Un registre des risques rassemble les informations concernant les risques afin d'informer les personnes exposées à ces risques et celles qui ont la responsabilité de leur gestion. Il peut s'agir d'un document papier ou d'une base de données, qui contient généralement:

- une brève description du risque (par exemple, un nom, les conséquences et la séquence d'événements qui mène aux conséquences, etc.);
- une déclaration concernant la vraisemblance que les conséquences surviennent;
- les sources ou les causes du risque;
- les actions actuelles visant à maîtriser le risque.

Les risques peuvent être classés en différentes catégories pour faciliter la création du rapport (B.2.2).

Les risques sont généralement répertoriés de manière individuelle comme des événements séparés, mais il convient de signaler les interdépendances.

En consignait les informations concernant les risques, il convient d'établir clairement la distinction entre les risques (les effets potentiels de ce qui pourrait se produire), les sources de risques (comment ou pourquoi cela pourrait se produire) et les moyens de maîtrise qui pourraient être défaillants. Il peut également être utile de mentionner les signes précurseurs indiquant que l'événement pourrait être imminent.

Souvent, les registres des risques contiennent également un classement d'importance du risque, une mention indiquant si un risque est réputé acceptable ou tolérable, ou si un traitement supplémentaire est nécessaire, ainsi que les raisons de cette décision. Si un classement d'importance est appliqué à un risque du fait de ses conséquences et de leur vraisemblance, il convient qu'il tienne compte de la possibilité de défaillance des moyens de maîtrise. Il convient de ne pas attribuer de niveau de risque à la défaillance d'un moyen de maîtrise comme s'il s'agissait d'un risque indépendant.

Les risques dont les conséquences sont positives peuvent être consignés dans le même document que ceux dont les conséquences sont négatives ou séparément. Les opportunités (c'est-à-dire les circonstances ou les idées qui pourraient être exploitées par opposition aux événements fortuits) sont généralement consignées séparément et analysées de manière à tenir compte des coûts, des avantages et de toute conséquence négative possible. Ce document peut parfois être appelé registre de la valeur et des opportunités.

B.10.2.2 Utilisation

Un registre des risques est utilisé pour consigner et pour tracer les informations concernant chaque risque et la manière dont il est contrôlé. Il peut être utilisé pour transmettre des informations concernant les risques pour les parties prenantes et pour mettre en évidence les risques particulièrement importants. Il peut être utilisé au niveau de l'organisation, du service, de l'opération ou du projet, où un grand nombre de risques, de moyens de maîtrise et de

traitements ont besoin d'être suivis. Les informations extraites d'un registre des risques peuvent être fusionnées pour fournir des informations à la haute direction.

Un registre des risques peut servir de base au suivi de la mise en œuvre des traitements suggérés, et peut donc contenir des informations concernant les traitements et la manière dont ils seront mis en œuvre, ou bien faire référence à d'autres documents ou bases de données qui contiennent ces informations. (Ces informations peuvent inclure les propriétaires de risques, les actions, les propriétaires des actions, les résumés des analyses de rentabilité des actions, les budgets et les délais, etc.). Une forme de registre des risques peut être exigée dans certaines situations.

B.10.2.3 Entrées

Les entrées d'un registre des risques sont généralement les résultats des techniques d'appréciation du risque décrites dans les Articles B.1 à B.4, complétés par l'historique des défaillances.

B.10.2.4 Résultats

Les résultats sont des archives d'informations et des rapports concernant les risques.

B.10.2.5 Avantages et limites

Les avantages des registres des risques incluent ce qui suit.

- Les informations concernant les risques sont rassemblées sous une forme qui permet d'identifier et de tracer les actions exigées.
- Les informations concernant les différents risques sont présentées dans un format comparable pouvant être utilisé pour indiquer les priorités et relativement facile à interroger.
- Habituellement, les personnes impliquées dans la construction d'un registre des risques sont nombreuses, ce qui permet une sensibilisation générale à la nécessité de gérer les risques.

Les limites incluent ce qui suit.

- Les risques collectés dans les registres des risques s'appuient habituellement sur des événements, ce qui peut compliquer la caractérisation exacte de certaines formes de risque (voir 4.2).
- L'apparente facilité d'utilisation peut rendre faussement confiant vis-à-vis des informations, car il peut être difficile de décrire les risques de manière cohérente et les confusions entre les sources de risques, les risques et les faiblesses des moyens de maîtrise du risque sont courantes.
- Les manières de décrire un risque sont nombreuses et la priorité allouée dépendra de la manière dont le risque est décrit et du niveau de désagrégation du problème.
- L'effort exigé pour maintenir un registre des risques à jour est considérable (par exemple, il convient d'intégrer tous les traitements suggérés à la liste des moyens de maîtrise en vigueur après leur mise en œuvre, d'ajouter continuellement les nouveaux risques et de supprimer ceux qui n'existent plus).
- Les risques sont habituellement collectés individuellement dans les registres des risques. Il peut donc être difficile de fusionner les informations pour développer un programme de traitement global.

B.10.2.6 Documents de référence

Aucun document de référence n'est disponible pour cette technique.

B.10.3 Matrice conséquence/vraisemblance (matrice de risque ou carte thermique)

B.10.3.1 Vue d'ensemble

La matrice conséquence/vraisemblance (également appelée "matrice de risque" ou "carte thermique") est une manière d'afficher les risques en fonction de leur conséquence et de leur vraisemblance, et de combiner ces caractéristiques afin d'afficher un classement d'importance du risque.

Des échelles de conséquence et de vraisemblance sur mesure sont définies pour les axes de la matrice. Les échelles peuvent contenir n'importe quel nombre de points (les échelles à trois, quatre ou cinq points sont les plus courantes) et elles peuvent être qualitatives, semi-quantitatives ou quantitatives. Si des descriptions numériques sont utilisées pour définir les graduations des échelles, il convient qu'elles soient cohérentes avec les données disponibles et que les unités soient données. D'une manière générale, pour être cohérent avec les données, chaque point des deux échelles nécessitera d'avoir un ordre d'amplitude supérieur au précédent.

L'échelle (ou les échelles) des conséquences peut (peuvent) représenter des conséquences positives ou négatives. Il convient de relier directement les échelles aux objectifs de l'organisation et de les étendre de la conséquence maximale crédible à la conséquence minimale considérée. Un exemple partiel pour les conséquences non souhaitables est représenté à la Figure B.15.

Caractéristique assignée	Financière	Hygiène et sécurité	Environnement et communauté	Etc.
a	Perte maximale crédible (\$)	Décès multiples	Important préjudice irréversible, outrage à la communauté	
b	⋮	⋮	⋮	⋮
c	⋮	⋮	⋮	⋮
d	⋮	⋮	⋮	⋮
e	Minimum considéré (\$)	Premiers secours exigés seulement	Dommages temporaires mineurs	

IEC

Figure B.15 – Exemple partiel de tableau définissant les échelles de conséquences

NOTE L'utilisation d'exemples partiels empêche l'utilisation directe des exemples, afin d'insister sur le fait qu'il convient toujours de personnaliser les échelles.

Des catégories supplémentaires ou moins de catégories peuvent être utilisées, et les échelles peuvent contenir plus ou moins de cinq points, selon le contexte. La colonne de classement des conséquences peut contenir des mots, des chiffres ou des lettres.

Il convient que l'échelle de vraisemblance couvre la plage pertinente pour les données concernant le risque à évaluer. Un exemple partiel d'échelle de vraisemblance est représenté à la Figure B.16.

Caractéristique assignée	Descripteur	Signification du descripteur
5	Probable	Attendu dans les prochaines semaines
4		
3		
2		
1	Vague possibilité	Possible en théorie, mais très improbable

IEC

Figure B.16 – Exemple partiel d'échelle de vraisemblance

L'échelle de classement de la vraisemblance peut contenir plus ou moins de cinq points et les rangs peuvent être donnés sous forme de mots, de chiffres ou de lettres.

Il convient d'adapter l'échelle de vraisemblance à la situation, et il peut être nécessaire qu'elle couvre une plage différente pour les conséquences positives et négatives. Si la conséquence la plus élevée est réputée tolérable selon une vraisemblance relativement faible, il convient que l'échelon le plus bas de l'échelle de vraisemblance représente une vraisemblance acceptable pour la conséquence ayant la définition la plus élevée (faute de quoi toutes les activités aux conséquences les plus élevées sont définies comme intolérables et ne peuvent pas devenir tolérables). Pour définir la vraisemblance tolérable d'un risque aux conséquences élevées seul, il convient de tenir compte du fait que plusieurs risques peuvent entraîner la même conséquence.

Une matrice est tracée, la conséquence et la vraisemblance étant placées sur leur axe respectif en respectant les échelles définies. Un classement de priorité peut être lié à chaque cellule. L'exemple présenté contient cinq rangs de priorité, indiqués ici par des chiffres romains. Les cases sont généralement associées à une couleur indiquant l'ampleur du risque. Les règles de décision (comme le niveau d'attention dans la gestion ou l'urgence de la réponse) peuvent être liées aux cellules de la matrice. Elles dépendront des définitions utilisées pour les échelles et de l'attitude de l'organisation face au risque. Il convient que la conception permette de fonder l'ordre de priorité d'un risque sur la mesure dans laquelle le risque mène à des résultats extérieurs aux seuils de performances définis par l'organisation pour ses objectifs.

La matrice peut être configurée pour donner une pondération supplémentaire aux conséquences (voir Figure B.17) ou à la vraisemblance, ou peut être symétrique, selon l'application.

↑ Classement des conséquences	a	III	III	II	I	I
	b	IV	III	III	II	I
	c	V	IV	III	II	I
	d	V	V	IV	III	II
	e	V	V	IV	III	II
		1	2	3	4	5
		→ Classement des vraisemblances				

IEC

Figure B.17 – Exemple de matrice conséquence-vraisemblance

B.10.3.2 Utilisation

Une matrice conséquence/vraisemblance est utilisée pour évaluer et pour communiquer l'amplitude relative des risques en fonction de la paire conséquence/vraisemblance habituellement associée à un événement central.

Pour classer les risques, l'utilisateur recherche en premier lieu le descripteur de conséquence correspondant le mieux à la situation, puis définit la vraisemblance d'occurrence de ces conséquences. Un point est placé dans la case qui combine ces valeurs, puis le niveau de risque et la règle de décision associée sont annoncés en fonction de la matrice.

Les risques ayant des conséquences potentiellement élevées sont souvent les plus inquiétants pour les décideurs, même lorsque la vraisemblance est très faible, mais les conséquences cumulées ou à long terme d'un risque fréquent dont l'impact est faible peuvent être élevées. Il peut être nécessaire d'analyser les deux types de risques, car les traitements du risque qui leur sont appliqués respectivement peuvent être tout à fait différents.

Lorsqu'il est possible qu'un même événement entraîne plusieurs valeurs de conséquence, la vraisemblance de toute conséquence particulière sera différente de la vraisemblance de l'événement à l'origine de cette conséquence. La vraisemblance de la conséquence spécifiée est généralement utilisée. Il convient que les modalités d'interprétation et d'utilisation de la vraisemblance soient cohérentes sur l'ensemble des risques comparés.

La matrice peut être utilisée pour comparer les risques ayant différents types de conséquences potentielles; elle a des applications à tous les niveaux d'une organisation. Elle est habituellement utilisée comme un outil de dépistage lorsque de nombreux risques ont été identifiés (pour définir les risques qu'il est nécessaire de signaler à un niveau hiérarchique plus élevé, par exemple). Elle peut également être utilisée pour aider à déterminer si un risque donné est largement acceptable ou inacceptable selon sa position dans la matrice. Elle peut être utilisée lorsque les données d'analyse détaillée ne sont pas suffisantes ou que la situation ne garantit pas le temps et les efforts nécessaires pour procéder à une analyse approfondie ou quantitative. Une forme de matrice conséquence/vraisemblance peut être utilisée pour l'analyse de criticité de la méthode AMDEC (B.2.3) ou pour définir les priorités à la suite d'une analyse HAZOP (B.2.4) ou SWIFT (B.2.6).

B.10.3.3 Entrées

Il est nécessaire que la mise au point d'une matrice conséquence/vraisemblance soit adaptée au contexte. Pour ce faire, certaines données sont exigées pour établir des échelles réalistes. Des projets de matrices nécessitent d'être soumis à essai afin de vérifier que les actions suggérées par la matrice correspondent à l'attitude de l'organisation face au risque et que les utilisateurs comprennent bien l'application des échelles.

L'utilisation de la matrice implique d'avoir à disposition des personnes (l'idéal serait une équipe) qui comprennent les risques à l'étude et toutes les données disponibles pour faciliter le jugement concernant les conséquences et leurs vraisemblances.

B.10.3.4 Résultat

Le résultat est un affichage représentant la vraisemblance relative et le niveau de risque des conséquences de différents risques, ainsi qu'un classement d'importance pour chaque risque.

B.10.3.5 Avantages et limites

Les avantages incluent ce qui suit.

- L'utilisation est relativement simple.
- Elle permet de classer rapidement les risques en différents niveaux d'importance.
- Elle offre un affichage visuel clair de l'importance d'un risque qui correspond à sa conséquence, à sa vraisemblance ou à son niveau de risque.
- Elle peut être utilisée pour comparer des risques ayant des conséquences de type différent.

Les limites incluent ce qui suit.

- Une bonne maîtrise est exigée pour pouvoir créer une matrice valable.
- Il peut être difficile de définir des échelles communes pour les appliquer à un éventail de circonstances pertinentes pour l'organisation.
- Il est difficile de définir les échelles sans ambiguïté afin de permettre aux utilisateurs de pondérer la conséquence et la vraisemblance de manière cohérente.
- La validité des classements de risques dépend de la qualité des échelles développées et de leur étalonnage.
- Une seule valeur indicative est exigée pour définir la conséquence, alors que dans de nombreuses situations, plusieurs valeurs de conséquence sont possibles et le classement du risque dépend de la valeur choisie.
- Une matrice étalonnée correctement contiendra des niveaux de vraisemblance très faibles pour de nombreux risques individuels qui sont difficiles à conceptualiser.
- Son utilisation est très subjective et différentes personnes attribuent souvent des classements très différents au même risque. Ceci l'expose à des manipulations.
- Il n'est pas possible d'agréger directement les risques (par exemple, il n'est pas possible de définir si un certain nombre de risques faibles, ou un risque faible identifié un certain nombre de fois, équivaut à un risque moyen).
- Il est difficile de combiner ou de comparer le niveau de risque de différentes catégories de conséquences.
- Pour être valable, un classement exige une formulation des risques cohérente (ce qui est difficile à obtenir).

- Chaque classement dépendra de la manière dont un risque est décrit et du niveau de détail donné (c'est-à-dire que plus l'identification est détaillée, plus le nombre de scénarios consignés est grand, et plus la vraisemblance de chacun est faible). Dans le cadre de la description du risque, il convient que la manière dont les scénarios sont regroupés soit cohérente et définie avant le classement.

B.10.3.6 Documents de référence

[89] ELMONSTRI, Mustafa, *Review of the strengths and weaknesses of risk matrices*

[90] BAYBUTT, Paul, *Calibration of risk matrices for process safety*

B.10.4 Courbes en S

B.10.4.1 Vue d'ensemble

Lorsqu'un risque peut avoir plusieurs valeurs de conséquence, elles peuvent être affichées sous la forme d'une distribution de la probabilité des conséquences (FDP). Voir par exemple la courbe continue de la Figure B.18. Les données peuvent aussi être relevées sous la forme d'une distribution cumulative (FDC), parfois appelée courbe en S (courbe en pointillés dans la Figure B.18). La FDP peut être paramétrique ou non paramétrique.

La probabilité qu'une conséquence dépasse une valeur particulière peut être annoncée directement à partir de la courbe en S. Par exemple, la Figure B.18 indique que la probabilité que les conséquences ne dépasseront pas la valeur de conséquence C est de 90 %.

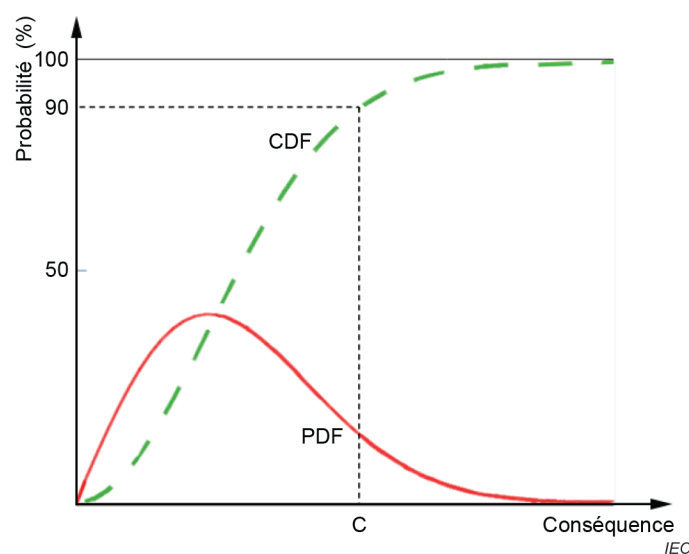


Figure B.18 – Fonction de distribution de la probabilité et fonction de distribution cumulative

Dans certains cas, la forme de la distribution est connue pour des raisons théoriques. Dans d'autres cas, la forme de la distribution peut être obtenue à partir de données, ou bien elle est le résultat d'un modèle.

Il est également possible d'utiliser le jugement d'un expert pour estimer le point le plus bas de l'éventail de conséquences, le centre probable et le point le plus haut de l'éventail. Plusieurs formules peuvent ensuite être utilisées pour déterminer la valeur moyenne des conséquences et la variance, et une courbe peut être tracée à partir de ces informations.

B.10.4.2 Utilisation

Une fdp indique la vraisemblance de différentes valeurs de conséquence sous une forme visuelle qui montre la valeur la plus probable, l'étendue de la variabilité et dans quelle mesure un événement extrême est probable.

Dans certaines circonstances, il peut être utile d'obtenir une seule valeur représentative au sein de la distribution de la probabilité, par exemple, pour la comparer aux critères d'évaluation. Souvent la valeur attendue (équivalente à la moyenne) est utilisée pour représenter la meilleure estimation de l'amplitude des conséquences. (Elle est équivalente à la somme des probabilités et de la conséquence représentée sur la courbe.) D'autres mesures comprennent la variance de la distribution ou une certaine plage de percentiles comme l'écart interquartile (la portion de l'échelle comprise entre le 25e percentile et le 75e percentile) ou le 5e et le 95e percentile (voir par exemple la VaR en B.7.2). Toutefois, l'accent mis par ces mesures sur la possibilité des conséquences extrêmes pourrait être encore insuffisant, alors qu'elles peuvent être importantes pour les décisions à prendre. Par exemple, pour choisir un investissement, le rendement attendu et les fluctuations de rendement sont pris en compte; pour prévoir les interventions en cas d'incendie, il est nécessaire de prendre en compte les événements extrêmes ainsi que les conséquences attendues.

La courbe en S est un outil utile pour examiner les valeurs des conséquences qui représentent un risque acceptable. La présentation des données permet de visualiser plus facilement la probabilité que les conséquences dépasseront une valeur particulière.

B.10.4.3 Entrées

La création d'une courbe en S exige des données ou des jugements pour pouvoir produire une distribution valable. Les distributions peuvent être produites à partir de jugements et avec peu de données, mais plus les données disponibles sont nombreuses, plus la distribution et les statistiques ainsi obtenues seront valides.

B.10.4.4 Résultats

Les résultats sont un diagramme qui peut être utilisé par les décideurs pour examiner l'acceptabilité d'un risque, et différentes statistiques déduites de la distribution qui peuvent être comparées aux critères.

B.10.4.5 Avantages et limites

Les avantages incluent ce qui suit.

- Cette technique représente l'amplitude d'un risque lorsque les conséquences sont distribuées.
- Les experts peuvent habituellement juger la valeur maximale, la valeur minimale et la valeur la plus probable de la conséquence, et produire une estimation raisonnable de la forme probable de la distribution. Un transfert sous la forme d'une distribution cumulative facilite l'utilisation de ces informations par les non-spécialistes. La précision de la courbe s'améliore à mesure qu'augmentent la quantité et la fiabilité des données d'entrée disponibles.

Les limites incluent ce qui suit.

- Cette méthode peut donner une impression d'exactitude qui n'est pas justifiée par le niveau de certitude des données à partir desquelles la distribution a été produite.

- Quelle que soit la méthode d'obtention d'une valeur ponctuelle ou de valeurs permettant de représenter une répartition des conséquences, il existe des hypothèses sous-jacentes et des incertitudes relatives:
 - à la forme de la distribution (par exemple, normale, discrète ou asymétrique);
 - au moyen le plus approprié de représenter cette répartition sous la forme d'une valeur ponctuelle;
 - à la valeur de l'estimation ponctuelle, compte tenu des incertitudes inhérentes aux données à partir desquelles elle est déduite.
- Les distributions et leurs statistiques en fonction de l'expérience ou des données antérieures fournissent toujours peu d'informations sur la vraisemblance des événements futurs ayant des conséquences extrêmes, mais une faible vraisemblance.

B.10.4.6 Document de référence

- [91] GARVEY, P., BOOK S.A., COVERT R.P. *Probability Methods for Cost Uncertainty Analysis: A Systems Engineering Perspective*

Bibliographie

Généralités

- [1] Principe "GAME" (*Globalement au moins équivalent*), *Méthodologie de démonstration, Les guides d'application*. Systèmes de transport public guidés urbains de personnes. 2011
- [2] FEKETE ISTVAN, *Integrated Risk Assessment for supporting Management decisions* Scholars Press, Saarbrücken, Germany 2015
- [3] PEACE, C. The reasonably practicable test and work health and safety-related risk assessments *New Zealand Journal of Employment Relations*. 2017, 42(2), 61-78

Techniques permettant de faire émerger les points de vue des parties prenantes et des experts

- [4] EN 12973, *Management par la valeur*
- [5] PROCTOR, A. *Creative problem solving for managers*. Abingdon: Routledge
- [6] GOLDENBERG, Olga, WILEY, Jennifer. Quality, conformity, and conflict: Questioning the assumptions of Osborn's brainstorming technique, *The Journal of Problem Solving*. 2011, 3(2), 96-108 [consulté 2019-02-13], disponible à l'adresse: <http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1093&context=jps>
- [7] ROWE, G. WRIGHT, G. The Delphi technique: Past, present, and future prospects. *Technological forecasting and social change*. 2011, 78, Special Delphi Issue
- [8] MCDONALD, D. BAMMER, G. and DEANE, P. *Research Integration Using Dialogue Methods*, ANU press Canberra. 2009 Chapter 3 Dialogue methods for understanding a problem: integrating judgements. Section 7: Nominal Group Technique [consulté 2019-02-13]. Disponible à l'adresse: <http://press.anu.edu.au/node/393/download>
- [9] HARRELL, M.C. BRADLEY, M.A. 2009 *Data collection methods – A training Manual – Semi structured interviews and focus groups*, RAND National defence research Institute USA [consulté 2019-02-13]. Disponible à l'adresse: http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR718.pdf
- [10] GILL, J. JOHNSON, P. *Research methods for managers* 4th ed. 2010 London: Sage Publications Ltd
- [11] SAUNDERS, M. LEWIS, P. THORNHILL, A. *Research Methods for Business Students* 7th ed. 2016 Harlow: Pearson Education Ltd
- [12] UNIVERSITY OF KANSAS COMMUNITY TOOL BOX Section 13 *Conducting surveys*; [consulté 2019-02-13]. Disponible à l'adresse: <https://ctb.ku.edu/en/table-of-contents/assessment/assessing-community-needs-and-resources/conduct-surveys/main>

Techniques d'identification du risque

- [13] MATHERLY, Carter *The Red Teaming Essential: Social Psychology Premier for Adversarial Based Alternative Analysis*. 2013 Disponible à l'adresse: <https://works.bepress.com/matherly/6/download/>

- [14] *Pestle analysis* Free Management E books [consulté 2019-02-13]. Disponible à l'adresse: <http://www.free-management-ebooks.com/dldebk/dlst-pestle.htm>
- [15] POPOV, G., LYON, B., HOLLICROFT, B., *Risk Assessment: A Practical Guide to Assessing Operational Risks*. Hoboken, NJ: Wiley, 2016
- [16] IEC 62740, *Analyse de cause initiale (RCA)*
- [17] BROUGHTON, Vanda. *Essential classification*. Facet Publishing 2015
- [18] BAILEY, Kenneth. Typologies and taxonomies: An introduction to classification technique. *Quantitative applications in the social sciences* Series 7,102 1994 Sage publications
- [19] VDI 2225 Blatt 1, *Konstruktionsmethodik- Technisch-wirtschaftliches Konstruieren - Vereinfachte Kostenermittlung*, 1997 Beuth Verlag
- [20] IEC 60812, *Analyse des modes de défaillance et de leurs effets (AMDE et AMDEC)*
- [21] IEC 61882, *Etudes de danger et d'exploitabilité (études HAZOP) – Guide d'application*
- [22] RINGLAND, Gill. *Scenarios in business*, Chichester: John Wiley, 2002
- [23] Van der HEIJDEN, Kees. *Scenarios: The art of strategic conversation*, Chichester; John Wiley, 2005
- [24] CHERMACK, Thomas J. *Scenario planning in organizations*, San Francisco: Berrett Koehler publishers Inc. 2011
- [25] MUKUL PAREEK, *Using Scenario analysis for managing technology risk* [consulté 2019-02-13]. Disponible à l'adresse: <http://www.isaca.org/Journal/archives/2012/Volume-6/Pages/Using-Scenario-Analysis-for-Managing-Technology-Risk.aspx>
- [26] CARD, Alan J. WARD, James R. and CLARKSON, P. John. Beyond FMEA: The structured what-if technique (SWIFT) *Journal of Healthcare Risk Management*, 2012, 31,(4) 23–29

Techniques de détermination des sources, causes et facteurs de risque

- [27] KERVERN, G-Y. *Elements fondamentaux des cindyniques*, Editions Economica 1995
- [28] KERVERN, G-Y. *Latest advances in cindynics*, Editions Economica, 1994
- [29] KERVERN, G-Y. & BOULENGER, P. *Cindyniques – Concepts et mode d'emploi*, Edition Economica 2007
- [30] ISHIKAWA, K. *Guide to Quality Control*, Asia Productivity Organization, 1986

Techniques d'analyse des moyens de maîtrise existants

- [31] LEWIS, S. SMITH, K., *Lessons learned from real world application of the bow-tie method. 6th AIChE. Global Congress of Process Safety*, 2010, San Antonio, Texas [consulté 2019-02-13]. Disponible à l'adresse: <http://risktec solutions.co.uk/media/43525/bow-tie%20lessons%20learned%20-%20aiche.pdf>

- [32] HALE, A. R., GOOSSENS L.H.J., ALE, B.J.M., BELLAMY L.A. POST J. *Managing safety barriers and controls at the workplace. In Probabilistic safety assessment and management*. Editors SPITZER C, SCHMOCKER, U, DANG VN,. Berlin: Springer; 2004. pp. 608–13
- [33] MCCONNELL, P. and DAVIES, M. *Scenario Analysis under Basel II*. [consulté 2019-02-13]. Disponible à l'adresse: <http://www.continuitycentral.com/feature0338.htm>
- [34] ISO 22000, *Systèmes de management de la sécurité des denrées alimentaires – Exigences pour tout organisme appartenant à la chaîne alimentaire*
- [35] *Systèmes de qualité et de sécurité sanitaire des aliments – Manuel de formation sur l'hygiène alimentaire et le Système d'analyse des risques – Points critiques pour leur maîtrise (HACCP)* [consulté 2019-02-13]. Disponible à l'adresse: <http://www.fao.org/docrep/W8088E/w8088e05.htm>
- [36] IEC 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*
- [37] IEC 61511 (toutes les parties), *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation*
- [38] CENTRE FOR CHEMICAL PROCESS SAFETY OF THE AMERICAN INSTITUTE OF CHEMICAL ENGINEERS New York 2001. *Layer of protection analysis – Simplified process risk assessment*

Techniques permettant de comprendre les conséquences et la vraisemblance

- [39] GHOSH, J., DELAMPADY, M. and SAMANTA, T. *An introduction to Bayesian analysis*, New York Springer-Verlag, 2006
- [40] QUIGLEY, J.L., BEDFORD, T.J. and WALLS, L.A. Prior Distribution Elicitation. In: *Encyclopaedia of Statistics in Quality and Reliability*. Wiley. 2008 ISBN 9780470018613
- [41] NEIL, Martin and FENTON, Norman. *Risk Assessment and Decision Analysis with Bayesian Networks*. CRC Press, 2012
- [42] JENSEN, F.V., NIELSEN T. D. *Bayesian Networks and Decision Graphs*, 2nd ed. Springer, New York, 2007
- [43] NICHOLSON, A., WOODBERRY O and TWARDY C, *The “Native Fish” Bayesian networks*. Bayesian Intelligence Technical Report 2010/3, 2010
- [44] NETICA TUTORIAL Introduction to Bayes Nets: What is a Bayes Net? [consulté 2019-02-13]. Disponible à l'adresse https://www.norsys.com/tutorials/netica/secA/tut_A1.htm
- [45] ISO/TS 22317, *Sécurité sociétale – Systèmes de management de la continuité d'activité – Lignes directrices pour l'analyse d'impact sur l'activité*
- [46] ISO 22301, *Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences*
- [47] ANDREWS J.D, RIDLEY L.M. 2002. Application of the cause consequence diagram method to static systems, *Reliability engineering and system safety* 75(1) 47-58. Disponible à l'adresse: <https://dspace.lboro.ac.uk/dspace-jspui/bitstream/2134/695/1/01-22.pdf> [consulté 2019-02-13]

- [48] NIELSEN D.S. The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis, Danish Atomic Energy Commission, RISO-M-1374, May 1971
- [49] IEC 62502, *Techniques d'analyse de la sûreté de fonctionnement – Analyse par arbre d'événement (AAE)*
- [50] IEC TR 63039:2016, *Probabilistic risk analysis of technological systems – Estimation of final event rate at a given initial state* (disponible en anglais seulement)
- [51] IEC 62508, *Lignes directrices relatives aux facteurs humains dans la sûreté de fonctionnement*
- [52] BELL Julie, HOLROYD Justin, *Review of human reliability assessment methods*. Health and Safety Executive UK, HMSO 2009 [consulté 2019-02-13]. Disponible à l'adresse <http://www.hse.gov.uk/research/rrpdf/rr679.pdf>
- [53] OCDE, Establishing the Appropriate Attributes in Current Human Reliability Assessment Techniques for Nuclear Safety, NEA/CSNI/R 2015 [consulté 2019-02-13]. Disponible à l'adresse: [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=NEA/CSNI/R\(2015\)1&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=NEA/CSNI/R(2015)1&docLanguage=En)
- [54] IEC 61165, *Application des techniques de Markov*
- [55] OXLEY, ALAN. Markov Processes in Management Science, published by Applied Probability Trust, 2011 [consulté 2019-02-13]. Disponible à l'adresse: <https://studylib.net/doc/8176892/markov-processes-in-management-science>
- [56] Guide ISO/IEC 98-3:2008/Suppl.1:2008, *Incertitude de mesure – Partie 3: Guide pour l'expression de l'incertitude de mesure (GUM:1995) – Supplément 1: Propagation de distributions par une méthode de Monte Carlo*
- [57] UE: Règlement général sur la protection des données (Journal officiel de l'Union européenne, 4 mai 2016)
- [58] ICO (Royaume-Uni): *Conducting privacy impact assessments code of practice* [consulté 2019-02-13]. Disponible à l'adresse: <https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf>
- [59] CNIL (FR), *Privacy Impact assessment (PIA)* [consulté 2019-02-13]. Disponible à l'adresse: <https://www.cnil.fr/en/privacy-impact-assessment-pia>

Techniques d'analyse des dépendances et des interactions

- [60] BRYSON, J. M., ACKERMANN, F., EDEN, C., & FINN, C. (2004). *Visible thinking unlocking causal mapping for practical business results*. Chichester: John Wiley & Sons
- [61] ACKERMANN, F, HOWICK, S, QUIGLEY, J, WALLS, L, HOUGHTON, T. Systemic risk elicitation: Using causal maps to engage stakeholders and build a comprehensive view of risks, *European Journal of Operational Research* 2014, 238(1), 290-299
- [62] CENTRE COMMUN DE RECHERCHE, COMMISSION EUROPÉENNE; *Cross-impact analysis* [consulté 2019-02-13]. Disponible à l'adresse: http://forlearn.jrc.ec.europa.eu/guide/2_design/meth_cross-impact-analysis.htm

Techniques utilisées pour produire une mesure du risque

- [63] ORGANISATION MONDIALE DE LA SANTÉ Boîte à outils d'évaluation des risques pour la santé humaine: Dangers chimiques. 2010 [consulté 2019-02-13]. Disponible à l'adresse:
<http://apps.who.int/iris/bitstream/10665/255614/1/9789242548075-fre.pdf?ua=1>
- [64] US EPA *Guidelines for ecological risk assessment* 1998 [consulté 2019-02-13]. Disponible à l'adresse:
https://www.epa.gov/sites/production/files/2014-11/documents/eco_risk_assessment1998.pdf
- [65] CHANCE, D., BROOKS, R. *An introduction to derivatives and risk management*, (9th ed.). Publié par Mason, Ohio: South-Western Cengage Learning 2013
- [66] THOMAS J. and PEARSON Neil D. *Value at risk*. *Financial Analysts Journal* 2000 56, 47-67
- [67] CHOUDHRY, M. *An introduction to Value at Risk*, Ed. 5, John Wiley and Sons, Chichester UK, 2013
- [68] *Value at Risk* New York University. [consulté 2019-02-13]. Disponible à l'adresse:
<http://people.stern.nyu.edu/adamodar/pdfiles/papers/VAR.pdf>

Techniques d'évaluation de l'importance d'un risque

- [69] UK HEALTH AND SAFETY EXECUTIVE, 2010a: *HID'S Approach To 'As Low As Reasonably Practicable' (ALARP) Decisions* [consulté 2019-02-13]. Disponible à l'adresse: <http://www.hse.gov.uk/risk/theory/alarpglance.htm>
- [70] UK HEALTH AND SAFETY EXECUTIVE, 2010b: *Guidance on (ALARP) decisions in control of major accident hazards (COMAH)*, [consulté 2019-02-13]. Disponible à l'adresse: http://www.hse.gov.uk/foi/internalops/hid_circs/permissioning/spc_perm_37/
- [71] UK HEALTH AND SAFETY EXECUTIVE, 2014: *Principles and guidelines to assist HSE in its judgments that duty-holders have reduced risk as low as reasonably practicable* [consulté 2019-02-13]. Disponible à l'adresse:
<http://www.hse.gov.uk/risk/theory/alarp1.htm>
- [72] AMERICAN INSTITUTE FOR CHEMICAL ENGINEERS: *Understanding and using F-N Diagrams: Annex A in Guidelines for Developing Quantitative Safety Risk Criteria*. New York. John Wiley 2009
- [73] EVANS, A. *Transport fatal accidents and FN-curves: 1967-2001*. Health and Safety Executive Research Report RR 073 [consulté 2019-02-13]. Disponible à l'adresse:
<http://webarchive.nationalarchives.gov.uk/20101111125221/http://www.rail-reg.gov.uk/upload/pdf/rr073.pdf>
- [74] *Pareto Chart, Excel Easy* [consulté 2019-02-13]. Disponible à l'adresse:
<http://www.excel-easy.com/examples/pareto-chart.html>
- [75] *Pareto Chart* [consulté 2019-02-13]. Disponible à l'adresse:
<http://www.uphs.upenn.edu/gme/pdfs/Pareto%20Chart.pdf>
- [76] IEC 60300-3-11, *Gestion de la sûreté de fonctionnement – Partie 3-11: Guide d'application – Maintenance basée sur la fiabilité*

- [77] MACKENZIE Cameron A. *Summarizing risk using risk measures and risk indices. Risk Analysis*, 34,12 2143-2163 2014

Techniques de choix parmi des options

- [78] KHOJASTEH, P, (2016). Application of benefit-cost-risk formula and key change indicators to meet project objectives [consulté 2019-02-19]. Disponible à l'adresse: <https://www1.bournemouth.ac.uk/sites/default/files/asset/document/Mon%205.1%20Khojasteh%20Pejman%20Risk.pdf>
- [79] The Green book, Appraisal and Evaluation in Central Government; 2011 Treasury Guidance LONDON: TSO London
- [80] ANDOSEH, S., et al. The case for a real options approach to ex-ante cost-benefit analyses of agricultural research projects. *Food policy* 44, 2014, 218-226 [consulté 2019-02-13]. Disponible à l'adresse: http://pdf.usaid.gov/pdf_docs/pnaec758.pdf
- [81] KIRKWOOD, CRAIG. Decision Tree Primer University of Arizona in *Decision Analysis and System Dynamics resources* 2002 [consulté 2019-02-13]. Disponible à l'adresse: <http://www.public.asu.edu/~kirkwood/DASTuff/decisiontrees/>
- [82] MYERSON, ROGER B., *Game Theory: Analysis of Conflict*, Harvard University Press, 1991
- [83] MAYNARD SMITH, JOHN *Evolution and Theory of Games*, Cambridge University Press 1982
- [84] ROSENHEAD, J. and MINGER, J. (Eds), *Rational Analysis for a Problematic World Revisited*, 2nd ed. Wiley, Chichester UK, 2001
- [85] EN 16271:2012, *Management par la valeur – Expression fonctionnelle du besoin et cahier des charges fonctionnel – Exigences pour l'expression et la validation du besoin à satisfaire dans le processus d'acquisition ou d'obtention d'un produit*
- [86] DEPARTMENT FOR COMMUNITIES AND LOCAL GOVERNMENT, *Multi-criteria analysis: a manual* 2009 [consulté 2019-02-13]. Disponible à l'adresse: <https://www.gov.uk/government/publications/multi-criteria-analysis-manual-for-making-government-policy>
- [87] RABIHAH MHD.SUM *Risk Management Decision Making*, 2001 [consulté 2019-02-13]. Disponible à l'adresse: <http://www.isahp.org/uploads/47.pdf>
- [88] VELASQUEZ, M., HESTER, P. An Analysis of Multi-criteria Decision Making Methods, *International Journal of Operations Research*, 10 (2), 55-66, 2013 [consulté 2019-02-13]. Disponible à l'adresse: http://www.orstw.org.tw/ijor/vol10no2/ijor_vol10_no2_p56_p66.pdf

Techniques d'enregistrement et de consignation

- [89] ELMONSTRI, Mustafa, *Review of the strengths and weaknesses of risk matrices*, Journal of Risk Analysis and Crisis Response, 4 (1), 49-57, 2014 [consulté 2019-02-13]. Disponible à l'adresse:
http://www.atlantis-press.com/php/download_paper.php?id=11718
 - [90] BAYBUTT, Paul, *Calibration of risk matrices for process safety. Journal of Loss Prevention in the Process Industries*, 38, 163-168, 2015
 - [91] GARVEY, P., BOOK S.A., COVERT R.P. *Probability Methods for Cost Uncertainty Analysis: A Systems Engineering Perspective*, Ed 2 Annex E Unravelling the S curve. CRC 2016
-

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch